نظرية الأعداد

منشورات جامعة دمشق
كلية العلوم

نظرية الأعداد

الدكتورة
دعد الحسيني
أستاذة في قسم الرياضيات

الدكتور
محمد بشير قابيل
أستاذ في قسم الرياضيات

جامعة دمشق

الفهرس

الباب الثاني

الفصل الثالث

المقدمة

بسم الله الرحمن الرحيم

اهتم الإنسان منذ القدم بالأعداد وخواصها واستخدمها في التعاملات البسيطة والاقتصادية قبل دراسة خصائصها وتبين البحوث التاريخية أن السومريين منذ 5700 قبل الميلاد قد مهروا باستخدام الأعداد وأن البابليين منذ حوالي(2000 ق .م)

اهتموا بدراسة خواص الأعداد وبرعوا بالحساب ولا يمكن أن ننسى أثر قدماء المصريين والهنود والصينيين في هذا المضمار . وقد ساهم الإغريق في إغناء هذا العلم . إذ اهتم فيثاغورث حوالي (500 - 580 ق .م) بدراسة الأعداد من وجهة نظر فلسفية ومن المعروف أنه قد سافر إلى بابل ومصر والهند لأخذ العلوم وبعد وفاته أنشئت جامعة الاسكندرية . ولعل من أوائل وأهم أعضائها اقليدس (300 ق .م) الذي ألف كتاب الأصول الذي يحتوي على 13 مقالة ثلاث منها في نظرية الأعداد ، حيث بحث في الأعداد الأولية وأثبت أن عددها غير منته، وبحث في التحليل إلى عوامل وأوجد خوارزمية لتعيين القاسم المشترك الأعظم لعددين . واشتهر بعد ذلك الرياضي ديوفانتس السكندري حوالي 250 م وترجع شهرته إلى كتابه "علم الحساب" .

اهتم العرب بنظرية الأعداد وكان لهم فيها باع كبير فالعالم ثابت بن قرة الحراني (ت 834 م) بحث في الأعداد التامة وأوجد صيغة للأعداد المتحابة ، والعالم ابن الهيثم (1041- 965 م)(432 - 354 هـ) قدم معياراً لمعرفة أولية عدد ، وأثبت المبرهنة التي تنتسب حالياً إلى ويلسون (والتفصيل في

الملحق(٢)) ، وشرح كتاب الأصول لأقليدس وأضاف الكثير من البراهين « في حل شكوك كتاب اقليدس في الأصول وشرح معانيه »

- **والعالم أبو بكر محمد بن الحسن الكرخي (ت 1029 م)** وضع كتاب" البديع في الحساب"
- **والعالم ابن البنّاء المراكشي (ت1321 م)** وضع كتاب " تلخيص أعمال الحساب" الذي شرحه هو في كتاب" رفع الحجاب عن وجوه أعمال الحساب" سنة 1302 م
- **والعالم الكبير غياث الدين جمشيد الكاشي (ت 1436 م)** ألّف كتاب "مفتاح الحساب"
- **والعالم الكبير كمال الدين الفارسي (ت1320 م)** وضع الكتاب القيم" تذكرة الأحباب في بيان التحاب ورفع الحجاب عن وجوه أعمال الحساب ".

أما في الغرب فقد ابتدأ الاهتمام بنظرية الأعداد بشكل واضح منذ عهد بييرفيرما « ***Pierre de Fermat*** » (1665 - 1601م) ومن أشهر من ساهم في تطويرها أولر « ***Euler*** » (1783 - 1707م) ولاغرانج (1813 - 1736م) وليجاندر " Legendre " (1833 - 1752 م) ودير خليه "Dirchlet " (1859- 1805 م) ولقد تأثرت نظرية الأعداد بالحاسوب وأثرت به مما أكسبها تقدماً جعلها في المقدمة بين علوم الرياضيات المعاصرة وخصوصاً بعد أن تبين أن لخصائص الأعداد أهمية بالغة في علم التعمية والتشفير (***cryptology***) ، وفي أمن المعلومات (***data security***) .

ويعمل في تطوير نظرية الأعداد في الوقت الحاضر علماء من معظم دول العالم. وما زال هناك مئات من المسائل المفتوحة في هذا العلم تنتظر حلولاً لها

حتى إنه ليقال : إن نشوء المسائل المفتوحة في نظرية الأعداد أسرع بكثير من حل المسائل المطروحة ولابد لنا أن نذكر ما قاله الرياضياتي غاوص:

"الرياضيات ملكة العلوم ونظرية الأعداد ملكة الرياضيات "

ويتضمن هذا الكتاب المواضيع الآتية :

قابلية القسمة في Z وتطبيقاتها – القواسم المشتركة والمضاعفات المشتركة – الأعداد الأولية – معادلات ديوفانتس – التطابقات – التطابقات الخطية – الدوال العددية (أو الحسابية) وبعض الدوال الخاصة – الجذور الأولية والأدلة .

نشكر كل من ساهم في إعداد هذا الكتاب ونأمل أن يجد فيه القارىء العربي متعة وفائدة ، ونسأل الله التوفيق .

المؤلفان

تمهيد

حول مبدأ الاستقراء الرياضي

٠-١ مبدأ الاستقراء الرياضي :

لا بد قبل البدء بموضوعات المقرر من عرض مبدأين هامين يكثر استخدامهما في إثبات مبرهنات هذا المقرر ؛ الأول هو مبدأ الترتيب الحسن أو (الجيد) *Well- ordering Principle* والثاني هو مبدأ الاستقراء الرياضي المنتهي *Mathematical Induction Principle*

١ - مبدأ الترتيب الحسن :

إذا كانت A مجموعة جزئية غير خالية من مجموعة الأعداد الصحيحة الموجبة Z^+ فإنه يوجد في A عنصر أصغر مما سواه- من جميع عناصرها- أي يوجد $a_0 \in A$ بحيث : $a_0 \le a$ ، $\forall a \in A$ « وهذا العنصر الأصغر وحيد » .

٢ - مبدأ الاستقراء الرياضي المنتهي :

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

تمرين مُمهِّد :

إذا أشرنا بالرمز S_n للمقولة :

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

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

$1^3+2^3 \overset{?}{=} (1+2)^2 \overset{?}{=} (\frac{2\times 3}{2})^2$ صحيحة ؟

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

سؤال جوابه نعم إذن تم المطلوب .

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

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

ويمكن أن ينص مبدأ الاستقراء الرياضي أو كما يسمى أحياناً مبدأ البرهان بالتدريج أو بالاستقراء على ما يلي :

إذا أردت إثبات صحة قضية(تتعلق بالمتغير الطبيعي n ولنرمز لها بالرمز S_n) من أجل أي عدد طبيعي $n \geq 1$ ما عليك إلا أن تقوم بالخطوتين التاليتين :

- تتوثق بدايةً من صحتها من أجل $n=1$ (خطوة البداية أو الخطوة الأساسية) ثم :
- • نفترض أنها (صحيحة من أجل $n=k$) وتبرهن 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 (يقـرأ الرمز $\overset{?}{=}$ هل يساوي) :

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

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

أو : $k^2+4k+4\overset{?}{=}k^2+4k+4$

والجواب نعم وتم المطلوب .

٠-٢ ثلاث ملاحظات هامة

- ملاحظة (١) :

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 :

١) التوثق من أن S_{n_0} صحيحة (خطوة البداية)

٢) **نفترض أن** S_k صحيحة من أجل $k \geq n_0$

ونبرهن بعدها أن S_{k+1} صحيحة (خطوة الاستقراء)

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

(لاحظ أنها صحيحة من أجل $n = 4$)

الحل :

الخطوة الأولى : $s_4 \quad : \quad 2^4 \overset{?}{\leq} 4!$

(الرمز $\overset{?}{\leq}$ يقرأ هل هو أصغر أو يساوي)

$$2^4 = 16 \overset{?}{\leq} 24$$

والجواب نعم والخطوة الأولى قد أنجزت . لننتقل إلى الخطوة الثانية

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

$$k \geq 4$$

لإثبات أن : $2^{k+1} \leq (k+1)!$

نقول إن :

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

أي

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

أو

$$2 \overset{?}{\leq} k+1$$

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

- ملاحظة (٢):

مبدأ الاستقراء الثاني ويبرهن أنه مكافىء للأول :

لإثبات صحة قضية S_n من أجل جميع قيم n المحققة للشرط $n \geq n_0$ حيث n_0 معلومة . مثلاً قد نحتاج إلى :

١ً) التوثق من أنها صحيحة من أجل $n = n_0$

٢ً) افتراض صحتها من أجل جميع قيم n المحققة للشرط $n \leq k$

ثم إثبات صحتها من أجل $n = k+1$.

<u>مثال:</u> لتكن لدينا المتتالية العددية المعرفة كما يلي :

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

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

الإثبات : الخطوة الأساسية : نلاحظ أن :

$$a_4 = a_3 + a_2 + a_1 \leq 27 + 9 + 3 = 39 \leq 3^4 = 81$$

فالعلاقة صحيحة . (لاحظ أن $a_4 = 3+2+1 = 6 \leq 81$)

خطوة الاستقراء :

لنفترض أن $a_n \leq 3^n$ 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 $n \in N$.

أمثلة

مثال (١) أثبت أن

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

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 : $\sum_{i=1}^{k+1} i = 1+2+3+....+k+(k+1) = S_k + (k+1)$

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

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

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

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

- ملاحظة (٣) :

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 العلاقة $\forall\; n \ge n_0$.

مثال هادف (٢) : أثبت أنه إذا كانت العبارة

$$S_k \;:\; \sum_{i=1}^{k} i = 1+2+3+....+k = \frac{(k^2+k+2)}{2}$$ صحيحة

فإن S_{k+1} صحيحة أي أن :

$$S_{k+1}=\frac{(k+1)^2+(k+1)+2}{2}=\frac{k^2+3k+4}{2}$$

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 $n=1$

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

ولما كان $1\neq 2$ فإن S_1 غير صحيحة

لنتساءل هل يمكن إيجاد قيمة ابتدائية n_0 بحيث أن S_{n_0} محققة

فنثبت صحة S_n $\forall\, n\geq n_0$ ؟

من أجل ذلك و بالاستفادة من المثال (١) نكتب

$\sum_{i=1}^{n_0} i=\frac{n_0\,(n_0+1)}{2}=\frac{n_0^2+n_0+2}{2}$ أي $n_0^2+n_0\overset{?}{=}n_0^2+n_0+2$ أي $0=2$ وهذا غير صحيح مما يدل على أنه لا توجد أي قيمة n_0 ابتدائية تصح من أجلها العلاقة S_n

مثال (٣) : أثبت أن

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

الحل : الخطوة الأساسية : نلاحظ أن

$$S_1 :\quad 1 = 1 = 1^2$$

$$S_2 :\quad 1+3 = 4 = 2^2$$

$$S_3 :\quad 1+3+5 = 9 = 3^2$$

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 $\forall\, n \in Z^{+}$

تمارين مساندة

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

حيث n عدد طبيعي

أ) $\sum_1 , \sum_2 , \sum_3 , \sum_4$

ب٢) برهن بالاستقراء أن $\sum_n = \dfrac{n(n+1)(2n+1)}{6}$

ثانياً : أثبت ما يلي بطريقة الاستقراء الرياضي :

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

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

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

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

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

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

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

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

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

الباب الأول

الفصل الأول : قابلية القسمة في z وتطبيقاتها

الفصل الثاني : القواسم المشتركة والمضاعفات المشتركة

الفصل الثالث : الأعداد الأولية

الفصل الرابع : معادلات ديوفانتس

الفصل الأول

قابلية القسمة في Z وتطبيقاتها

- خواص قابلية القسمة
- مبرهنة اقليدس

١ – ١ قابلية القسمة في Z وتطبيقاتها :

١-١-١ 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 لـــ b و نـــسمي 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 : $3|15$ ، $5 \nmid 12$

١-١-٢ خواص قابلية القسمة :

١) يلاحظ من التعريف مباشرة أن العدد 1 هو قاسم لأي عدد صحيح ، وأن الصفر هو مضاعف لأي عدد صحيح .

٢) إذا كان a/b فإن $-a/b$

٣) $a/a \quad \forall a \neq 0$ لأن $a = 1.a$

٤) $a|c \Rightarrow a|kc \quad \forall k \in Z$

٥) $a|c \wedge c|d \Rightarrow a|d$

لأن

$$c = ab_1 \wedge d = cb_2 \Rightarrow d = a\,b_1b_2 = a(b_1b_2)$$

٦)

$$a|c \wedge a|d \Rightarrow a|(mc+nd) \quad \forall m,n \in Z$$

لأن

$$c = ab_1 \wedge d = ab_2 \Rightarrow mc+nd = ma\,b_1 + na\,b_2 = a(m\,b_1 + nb_2)$$

٢- ملاحظة :

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

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

٧) $a|c \quad \wedge \quad c \neq 0 \quad \Rightarrow \quad |a| \leq |c|$

لأن : $c = ab \neq 0 \quad \Rightarrow \quad |c| = |a|.|b| \quad \Rightarrow |c| \geq |a|$

٨) $a|c \quad \wedge \quad c|a \quad \Leftrightarrow \quad |a| = |c|$ لأن حسب الخاصة (٧)

$$|a| \leq |c| \quad \wedge \quad |c| \leq |a| \quad \Leftrightarrow \quad |a| = |c|$$

- نتيجة :

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

١-١-٣ 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 $b = a\,q + r$ 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 :

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

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 أنه يوجد r_1, q_1 يحققان العلاقة

$$b = q_1 a + r_1 \quad 0 \le r_1 < |a|$$

ولدينا

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

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	$56 = (-7)(-8) + 0$

١-١-٤ تطبيق هام :

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

الإثبات : إن باقي قسمة أي عدد فردي على العدد 2 يساوي 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 $q+1$ عددين متتاليين فإن أحدهما زوجي والآخر فردي

ومنه $b^2 = 8M+1$

تمرين (١) : أثبت أن $6 | 5m^3 + 7m$ حيث $m \in N$

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

الخطوة الأساسية :

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

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

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

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 (٦) فإن 6 تقسم المجموع $15k(k+1) + 12$

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

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

تمرين (٢) : أثبت أن $14 \mid 5^{2n+1} + 3^{4n+2}$ حيث $n \geq 0$

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

بطريقة الاستقراء :

١- الخطوة الأساسية : نلاحظ أن $14 \mid 14$, $f(0) = 14$ والعلاقة صحيحة.

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

لذا نحسب المقدار :

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

نصلح العلاقة الأخيرة فنجد :

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

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

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

بما أن $14 \mid f(k)$ فإن $14 \mid 11 f(k)$

ينتج أن $14 \mid f(k+1)$ وخطوة الاستقراء صحيحة أي أن :

$14 \mid f(n)$ عندما $n \geq 0$.

الفصل الثاني

القواسم المشتركة والمضاعفات المشتركة

- القاسم المشترك الأعظم وخواصه
- خوارزمية القسمة
- القاسم المشترك الأعظم لمجموعة أعداد صحيحة
- المضاعف المشترك الأصغر

١-٢ القواسم المشتركة والمضاعفات المشتركة

١-٢-١ تعريف : نقول إن العدد الصحيح $d_1 \neq 0$ قاسم مشترك للعددين الصحيحين a , b غير الصفرين معاً إذا تحقق ما يلي :

$$d_1 | b \quad \wedge \quad d_1 | a$$

مثلاً : $3|30$, $3|12$

١-٢-٢ ملاحظات :

- يلاحظ أنه إذا كان d_1 قاسماً مشتركاً لـــ a , b فإن $(-d_1)$ يكون قاسماً مشتركاً لهما أيضاً
- 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 $|b|$ و $|a|$
- 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 .

١-٢-٣ 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 : ١) $d > 0$

٢) $d | b \quad \wedge \quad d | a$

٣) إذا كان العدد الصحيح $c > 0$ و $c | a \quad \wedge \quad c | b$ 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 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 (٣) يمكن أن نكتب أن :

$$d_1 \le d_2 \wedge d_2 \le d_1 \Rightarrow d_1 = d_2$$

وهو المطلوب .

- **ملاحظة :** إن مجموعة القوا سم المشتركة 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 .

١-٢-٤ **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 :

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

إن المجموعة S غير خالية فهي تحوي :

$n = \pm a$ عندما $y = 0$, $x = \pm 1$

$n = \pm b$ عندما $y = \pm 1$, $x = 0$

أي أنها تحوي أعداداً موجبة وأعداداً سالبة .

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

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 :

$$n = n_0 q + r \qquad : \qquad 0 \le r < n_0 \qquad (١)$$

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

ولما كان $r \ge 0$ وهو تركيب خطي لـ b , a 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 (١) $r < n_0$ وهذا تناقض إذاً لابد وأن تكون $r = 0$ و $n_0 | n$ أي أن n_0 تقسم جميع عناصر S وبما أن كلاً من a , b عنصر من S فإن $n_0 | a$ و $n_0 | b$ أي n_0 قاسم مشترك للعددين b , a ومنه : $n_0 \le d = (a , b)$.

ومن جهة أخرى فإن العلاقة $n_0 = x_0 a + y_0 b$ تدل على أن كل قاسم لـ b , a 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 (١)** : يلاحظ مما سبق أن القاسم المشترك الأعظم لعددين غير معدومين هو العنصر الأصغر في مجموعة التراكيب الخطية الموجبة للعددين b , a .

- **ملاحظة (٢)** : إن تمثيل القاسم المشترك الأعظم لعددين كتركيب خطي ليس وحيداً .

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

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

أو $3 = 15(5) + 24(-3)$ .....

- **نتيجة :** إذا كان $d = (a, b)$ وكان c قاسماً مشتركاً لـ b, a

فإن $c|d$

الإثبات : حسب المبرهنة السابقة نكتب $d = x_0 a + y_0 b$

فإذا كان $c|a \wedge c|b$ فإن $c|d$

١-٢-٥ تعريف : إذا كان القاسم المشترك الأعظم لعددين صحيحين b, a يساوي الواحد فإننا نسمي العددين عددين أولين نسبياً (*relatively prime*)

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

١-٢-٦ مبرهنة : يكون العددان b, a غير المعدومين أوليين نسبياً فيما بينهما إذا وفقط إذا وجد عددان صحيحان x, y بحيث يكون :

$$a x + b y = 1$$

الإثبات : إذا كان $(a, b) = 1$ فحسب المبرهنة (١-٢-٤) نجد أن

$$1 = a x + b y \qquad x, y \in Z$$

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

أي $d|1$ ومنه $d = 1$

- **نتيجة :** إذا كان $(a, b) = d$ وكان $a = a_0 d \wedge b = b_0 d$

فإن $(a_0, b_0) = 1$.

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

وحسب المبرهنة (١-٢-٦) يكون $(\frac{a}{d}, \frac{b}{d}) = 1$ أي $(a_0, b_0) = 1$

١-٢-٧ بعض خواص القاسم المشترك الأعظم :

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

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

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

الإثبات : بما أن $(a,m)=1$ يمكن إيجاد عددين صحيحين y,x بحيث $ax+my=1$ نضرب طرفي العلاقة بـــ b فنجد :

$ab.x+mby=b$ لذا فإن أي قاسم d_1 لـــ ab و m يجب أن يقسم b أي :

$$d_1 \mid m \wedge d_1 \mid ab \Rightarrow d_1 \mid b$$

أصبح لدينا $d_1 \mid (b,m)$ أي $d_1 \mid 1$ ومنه $d_1=1$

٤) إذا كان $(k,b)=1$ و $k \mid ab$ فإن $k \mid a$

الإثبات : يمكن أن تكتب $1=kx+by$ نضرب الطرفين بـــ a فنجد :

$$a=ak.x+aby$$

لما كان k قاسماً لـــ ab وقاسما لـــ akx فهو يقسم مجموعهما a .

- **ملاحظة :** إذا كان $k \mid ab$ و $(k,b)\neq 1$ فإن k قد لا يقسم أياً من b , a

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

٥) إذا كان $(a,b)=1$ و $a \mid n$ و $b \mid n$ فإن $a.b \mid n$

الإثبات : نكتب $n=an_0$ ولدينا $b \mid n$ أي $b \mid an_0$

ولكن $(a,b)=1$ ومنه $b \mid n_0$ بالتالي يمكن أن نكتب $n_0=bm$

بتعويض n_0 بما يساويها في عبارة n نجد: $n = a\ b\ m$ أي أن $a\ b \mid n$

٦) إذا كان m عدداً صحيحاً موجباً وكان $(a\ ,b) = d$

فإن $D = (ma\ ,m\ b) = m\ d$

الإثبات : بما أن $(a\ ,b) = d$ نكتب $d = a\,x + b\,y$ نضرب الطرفين بـــ m

فنجد : $md = m\,a\ x + m\,b\,y$

ولدينا $D \mid ma$ و $D \mid mb$ ومنه نجد $D \mid md$ *

ومن جهة أخرى يمكن أن نكتب $D = m\,a\ x_1 + m\,b\,y_1$

ولدينا $d \mid b$ و $d \mid a$ حسب النظرية (١-٤-٦) نجد : $d \mid (ax_1 + by_1)$

ومنه $m\,d \mid m\,(a\,x_1\ ,\ b\,y_1)$ وهكذا نجد : $m\,d \mid D$ **

ومن * و** نجد أن $m\,d = D$.

- **تمهيدية :** إذا كان $0 \le r < a$, $b = q\,a + r$ فإن $(a,b) = (a,r)$

الإثبات : ليكن $(a,b) = d$ أي $d \mid a$ و $d \mid b$ ومنه $d \mid b - q\,a$

أي $d \mid r$ فهو قاسم مشترك لـــ $r\ ,a$.

ليكن c قاسماً للعددين $r\ ,a$ من الواضح أن $c \mid qa + r$ أي $c \mid b$ بما أن $c \mid a$ فإن $c \mid d$ بالتالي $c \le d$ أي $d = (a,r)$

- **خوارزمية اقليدس (*Euclidean algorithm*) :**

هي وسيلة لإيجاد القاسم المشترك الأعظم لعددين صحيحين .

نعلم أن $(a,b) = (|a|,|b|)$ لـــذا نفتـــرض أن $b \ge a > 0$ ونـــشرح الخوارزمية كما يلي :

نجري عمليات القسمة المتتالية : $b = q_1\,a + r_1$, $0 \le r_1 < a$

فإذا كانت $r_1 = 0$ فإن $(a,b) = (a\ ,0) = a$ وإذا كان $r_1 \ne 0$ نتابع القسمة :

$$a = q_2\ r_1 + r_2 \qquad , \quad 0 \le r_2 < r_1$$

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 بشكلٍ متتالٍ 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 (12378 , 3054)

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

أي $gcd\ (12378\ , 3054) = 6$

- **ملاحظة (١) :** يلاحظ من خوارزمية اقليدس أن البواقي المتتالية يمكن أن تكتب كتركيب خطي للعددين $a\ ,\ b$ حيث نجد :

$$r_1 = a - q_1\, b$$

$$r_2 = b - r_1\, q_2 = -q_2\, a + (1 + q_1\, q_2)\, b$$

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

$$
\begin{aligned}
6 &= 24 - 18 \\
&= 24 - (138 - (5).(24)) \\
&= (6).(24) - 138 = 6(162 - 138) - 138 \\
&= (6).(162) - (7).(138) = (6).(162) - 7(3054 - (18).162) \\
&= (132).(162) \quad (7).(3054) \\
&= 132(12378 - (4).(3054)) - (7).(3054) \\
&= 132(12378) + (-535)(3054)
\end{aligned}
$$

ومنه :

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

- **ملاحظة (٢) :**

يمكن الاستفادة من خواص القاسم المـــشترك الأعظـــم بتبـــسيط خطـــوات خوارزمية اقليدس وعلى سبيل المثال يمكن أن نكتب :

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

١-٢-٨ 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 :

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

إذا وفقط إذا كان : (١) $d>0$

(٢) $d \mid a_i \qquad 1\le i\le n$

(٣) إذا كان $c \mid a_i \qquad 1\le i\le n$ 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 $d \mid a_i$ $\quad i = 1, 2, \ldots, n$ أي

$$d \mid (a_{n-1}, a_n)$$

ومنه $d \mid d_1$ ومن جهة أخرى $d_1 \mid a_i$ $\quad i = 1, 2, \ldots, n-2$ و

$d_1 \mid (a_{n-1}, a_n)$ أي $d_1 \mid a_n$ و $d_1 \mid a_{n-1}$ ومنه $d_1 \mid a_i$ $\quad i = 1, 2, \ldots, n$

ومنه $d_1 \mid d$ بالتالي نجد $d = d_1$

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

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

مثال(١) : إن الأعداد $6, 14, 21$ أولية نسبياً لأن : $(6, 14, 21) = 1$

ولكنها ليست أولية نسبياً مثنى مثنى لأن :

$$(14, 21) = 7, \quad (6, 21) = 3, \quad (6, 14) = 2$$

مثال(٢) : إن الأعداد $6, 25, 77$ أولية نسبياً مثنى حيث

وهي أولية نسبياً لأن :

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

١-٢-٩ المضاعف المشترك الأصغر (least common multiple)

- **تعريف :** لتكن a_i حيث $i=1,...,n$ أعداداً صحيحةً غير صفرية

نقول إن m مضاعف لهذه الأعداد إذا كان $a_i | m$, $\forall\ i=1,...,n$

ونقول إن L هو المضاعف المشترك الأصغر لها ونكتب

$$lcm(a_1.....a_n)=L$$

إذا وفقط إذا كان :

(١) $L>0$

(٢) $\forall\ i=1,2,....,n \quad a_i \mid L$

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

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

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

- **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 : $0 \le r < L$: $m=qL+r$

ومنه $r=m-qL$ ، لدينا $a_i \mid m$, $a_i \mid L$ $\forall\ i=1,2,....,n$

ومنه نجد $a_i \mid r$ و $r<L$ وبما أن L هو العنصر الأصغر لمجموعة المضاعفات المشتركة الموجبة فإن $r=0$ حصراً و $L \mid m$

مبرهنة : إذا كان b , a عددين صحيحين موجبين وكان $d = gcd(a,b)$ و $L = \frac{a.b}{d}$ فإن $L = l.c.m(a,b)$

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 b , a ، ليكن m مضاعفاً مشتركاً لـــ a , b فـيمكن أن تكتب

$$m = a_1 a = a_1 a_0 d \ , \ b \mid m \Rightarrow b \mid a_1 a_0 d$$

ومنه

$$b_0 d \mid a_1 a_0 d \Rightarrow b_0 \mid a_1 a_0$$

ولما كان $(a_0, b_0) = 1$ فإن $b_0 \mid a_1$ أي $b_0 a \mid a_1 a = m$

أي $L \mid m$ و $L \le m$ ومنه L هو المضاعف المشترك الأصغر

- نتيجة : $L = a.b$ إذا كان $(a,b) = 1$

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

$d = (6,21) = 3$ ومنه $L = 42$

تمارين

١- استخدم طريقة الاستقراء الرياضي لإثبات ما يلي :

$15 \mid 2^{4n}$ $n \geq 0$ ، $7 \mid 2^{3n}-1$ $n \geq 1$

$8 \mid 3^{2n}$ $n \geq 0$ ، $8 \mid 3^{2n}+7$ $n \geq 1$

$23 \mid 4^{2n+1}$ 49 $n \geq 06$ ، $3 \mid 2^{n}+(-1)^{n+1}$ $n \geq 1$

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

$14 \mid 15x^2 -$

$49 \mid 24x^2 +$

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

$(a+b$

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

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

٥- هل العبارات التالية صحيحة أو خاطئة إن كانت أثبت صحتها وإن كانت خاطئة أعط مثالاً يبين ذلك :

١) إذا كان $a \mid b$ و $a \mid c$ $a^2 \mid bc$

٢) $a \mid b \Leftrightarrow ac \mid bc$ ، $c \neq 0$

٣) إذا كان $a \mid b+c$ فإن إما $a \mid b$

٤) إذا كان $a \mid b^2+1$ فإن $+1$

٥) إذا كان $a^2 \mid b^3$ فإن $a \mid b$

٦) إذا كان $a^2 \mid n \wedge b^2 \mid n$ فإن $a \mid b$

مبرهنة : إذا كان a , b عددين صحيحين موجبين وكان $d = gcd(a,b)$

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

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 لـــ a , b فـيمكن أن تكتب

$$m= a_1 a = a_1 a_0 d \quad , \quad b \mid m \quad \Rightarrow b \mid a_1 a_0 d$$

ومنه

$$b_0 d \mid a_1 a_0 d \qquad \Rightarrow b_0 \mid a_1 a_0$$

ولما كان $(a_0,b_0)=1$ فإن $b_0 \mid a_1$ أي $b_0 a \mid a_1 a = m$

أي $L \mid m$ و $L \le m$ ومنه L هو المضاعف المشترك الأصغر

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

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

$d=(6,21)=3$ ومنه $L=42$

تمارين

١- استخدم طريقة الاستقراء الرياضي لإثبات ما يلي :

$7 \mid 2^{3n}-1 \quad n\geq 1$ ، $15 \mid 2^{4n}-1 \quad n\geq 0$

$8 \mid 3^{2n}+7 \quad n\geq 1$ ، $8 \mid 3^{2n}+7 \quad n\geq 0$

$3 \mid 2^{n}+(-1)^{n+1} \quad n\geq 1$ ، $2304 \mid 7^{2n+2}-48n-49 \quad n\geq 06$

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

$14 \mid 15x^2-11x+14$

$49 \mid 24x^2+4x+41$

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

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

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

٥- هل العبارات التالية صحيحة أو خاطئة إن كانت صحيحة فأثبت صحتها وإن كانت خاطئة أعط مثالاً يبين ذلك :

١) إذا كان $a \mid b$ و $a \mid c$ فإن $a^2 \mid bc$

٢) $a \mid b \Leftrightarrow ac \mid bc$ حيث $c\neq 0$

٣) إذا كان $a \mid b+c$ فإن إما $a \mid b$ أو $a \mid c$

٤) إذا كان $a \mid b^2+1$ فإن $a \mid b^4+1$

٥) إذا كان $a^2 \mid b^3$ فإن $a \mid b$

٦) إذا كان $a^2 \mid n \wedge b^2 \mid n \wedge a^2 \leq b^2$ فإن $a \mid b$

٦- عين القاسم المشترك الأعظم :

$(227 , 659)$, $(143 , 227)$, $(306 , 657)$, $(272 , 1479)$

$(25 , 72 , 175 , 168)$, $(227 , 659 , 454)$, $(272 , 24 , 306)$

٧- أوجد قيماً لـــ y, x تحقق ما يلي

$$g.c.d\,(56 , 72) = 56\,x + 72\,y$$

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

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

٨- أوجد $lcm(143, 227)$ $lcm(272 , 1479)$

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

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

١٠- إذا كان : $f(n) = 7^{2n+2} - 48\,n - 49$ أثبت أن

$$n \geq 0 \quad 2304 \mid f(n)$$

الفصل الثالث

الأعداد الأولية

- الأعداد الأولية وخواصها
- المبرهنة الأساسية في الحساب
- مبرهنة الأعداد الأولية
- التحليل إلى عوامل بطريقة فيرما

١-٣ الأعداد الأولية (*Prime numbers*)

١-٣-١ تعريف: نقول إن العدد الصحيح p عدد أولي إذا تحقق ما يلي :

١- $p > 1$

٢- p لا يقبل القسمة إلا على نفسه وعلى العدد 1

ونسمي العدد الصحيح الموجب غير الأولي والأكبر تماماً من الواحد عدداً مؤلفاً (*composite number*)

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

حيث $1 < a < n$, $1 < b < n$.

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

١-٣-٢ بعض خواص الأعداد الأولية :

١- الأعداد الأولية هي أعداد أولية نسبياً مثنى مثنى .

٢- إذا كان العدد الأولي p يقسم العدد الصحيح n فإن $(p, n) = p$

فيما عدا ذلك فإن $(p, n) = 1$.

٣- إذا كان p عدداً أولياً وكان $p | a\,b$ فإن p يقسم أحدهما على الأقل أو بعبارة أخرى إذا كان $p \nmid a$ و $p | a\,b$ فإن $p | b$

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

٥- إذا كانت $p, p_1, p_2, ..., p_n$ أعداداً أولية وكان $p | p_1 \cdot p_2 ..... p_n$ فإن p يساوي أحد الأعداد الأولية p_i .

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

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

إن أي عدد صحيح $n > 1$ هو إما عدد أولي أو هو جداء 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

$n = 4 = 2 . 2$ ، $n = 5$ 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 فيمكن كتابته على النحو : $k + 1 = a . b$ حيث

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

ولما كان كلّ من a و b أصغر من $k + 1$ فهو يكتب كجداء عدد منته من العوامل الأولية 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 $2 = 2$ ، $6 = 2 . 3$ 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

$$k + 1 = p_1 . p_2 \dots p_s = q_1 . q_2 \dots q_t$$

من العلاقة الأخيرة ينتج أن $p_1 \mid q_1 . q_2 ..... q_t$

أي أن p_1 تساوي أحد الأعداد الأولية q_i ولـيكن $p_1 = q_j$. نغيـر ترتيـب العوامل q_i بحيث $q_j = q_1 = p_1$ ونكتب

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

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

أي أن تمثيل n_1 كجداء عوامل أولية تمثيل وحيد مما يدل علـى 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 أمكننـا كتابـة العـدد n كجداء عوامل أولية بالشكل القانوني كما يلي :

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

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

مثال :

$$360 = 2^3 . 3^2 . 5$$

$$17640 = 2^3 . 3^2 . 5 . 7^2$$

نتيجة (١) : كل عدد صحيح $n > 1$ له عامل أولـي أي يوجدعـدد أولـي p بحيث $p \mid n$.

نتيجة (٢) : إذا كان $n > 1$ عدداً مؤلفاً فله عامل أولي p بحيث يكون $p \le \sqrt{n}$.

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

$1 < a \le b < n$ ومنه $n = a.b \ge a^2$

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

أي $p \le \sqrt{n} \Leftarrow p \le a \;,\; p \mid n \Leftarrow p \mid a$

وهو المطلوب .

نتيجة (٣) : إذا كان $n > 1$ وليس له عامل أولي $\sqrt{n} \geq$ فإن n عدد أولي .

الإثبات :

ذلك أنه إذا لم يكن n أولياً كان عدداً مؤلفاً و إذا كان n عدداً مؤلفاً فله عامل أولي $\sqrt{n} \geq$ وهذا خلف

أي إذا كان $n > 1$ فهو إما عدد أولي أو له عامل أولي p يحقق $p \leq \sqrt{n}$.

- كم هو عدد الأعداد الأولية ؟!

شغلت هذه المسألة أذهان علماء الرياضيات منذ القدم وقد وضعت 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 $p \mid N$

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

$$p \mid 1 \Leftarrow p \mid N - p_1\, p_2 \ldots p_n \Leftarrow p \mid N \quad , \quad p \mid p_1\, p_2 \ldots p_n$$

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 $N_1 = 3$ ، $N_2 = 7$ ، $N_3 = 31$ ، $N_4 = 211$ ، $N_5 = 2311$ كلها أولية ولكن لسوء 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 خاطئ ، من هذه الصيغ :

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

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

ثم أثبت **غولدباخ** (1752) أنه لا توجد أي حدودية صحيحة 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 .

٣- 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 أو غربال **ايراتوستين** (***The sieve of Eratosthenes***) في القرن الثالث قبل الميلاد وسنشرح هذه الطريقة فيما يلي :

نكتب 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 $p \le \sqrt{N}$ 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 ١٧٩٣ ولم يتم إثباتها بشكل كامل ومبسط حتى عام ١٩٤٩ من قبل سيليرغ (*A . Sell erg*) و ايردوس (**P. *Erodes***)

مبرهنة الأعداد الأولية :

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

تمرين : احسب العددين $\pi(1000)$ و $\frac{1000}{Log1000}$ وقارن بينهما

احسب العددين $\pi(2000)$ و $\frac{2000}{Log2000}$ وقارن بينهما

استخدم الحاسوب حتى تصل إلى حساب $\pi(10^4)$ و $\frac{10^4}{Log10^4}$ وقارن بينهما

١-٣-٣ 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 ميرسن 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 و b 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 :

$$n = a\,b = \left(\frac{a+b}{2}\right)^2 - \left(\frac{a-b}{2}\right)^2$$

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 $k^2 - n$, $(k+1)^2 - n$ ..... 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 $n = n \cdot 1$ 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 (١) : 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 (٢) : لنحلل العدد $n = 315$ بطريقة فيرما

نلاحظ $17^2 < 315 < 18^2$ ونكتب

$$18^2 - n = 9 = 3^2$$

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

ونحلل كلاً من 15 و 21 فنجد $n = 315 = 3^2 . 5 . 7$

مثال (٣) : لنحلل العدد $n = 119143$

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 .

تمارين

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

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

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

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

٥- أوجد جميع الأعداد الأولية التي هي ≤ 30 .

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

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

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

٩- حلل الأعداد التالية إلى عواملها الأولية بطريقة فيرما :

945 , 977 , 2931 , 493 , 10541 , 31623

81518057 , 38025 , 2279 , 430663

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

الفصل الرابع

معادلات ديوفانتس

- معادلات ديوفانتس
- معادلات ديوفانتس الخطية بمجهولين
- ثلاثيات فيثاغورث

١-٤ معادلات ديوفانتس *Diophantus Equations*

١-٤-١ تمهيد : هي المعادلات التي سماها العرب المعادلات السيالة أي لها عدد لانهائي من الحلول وهي معادلات بعدة متحولات تخرج بصوابات (بأجوبة) 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 ، ويجد الحلول الصحيحة لها .

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

١-٤-٢ معادلات ديوفانتس الخطية بمجهولين :

نكتب هذه المعادلات على النحو : $ax + by = n$ 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 $(4,1)$, $(-6,6)$, $(10,-2)$ تحقق المعادلة $3x + 6y = 18$

وقد لا يكون لمثل هذه المعادلات أي حل ، فعلى سبيل المثال المعادلة $2x + 10y = 17$ 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 .

١-٤-٣ مبرهنة : إذا كان لدينا المعادلة (١) $ax + by = c$ حيث

$a, b, c \in Z$ و a , b غير معدومين 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 :

$$x = x_0 + \frac{b}{d} t$$

$$y = y_0 - \frac{a}{d} t$$

حيث t عدد صحيح ما .

البرهان : تعلم أنه إذا كان $d = (a, b)$ فيمكن إيجاد عددين صحيحين r , s بحيث يكون: $(r, s) = 1$, $a = r d$, $b = s d$.

فإذا وجد للمعادلة (١) حل وليكن x_0 , y_0 فإن :

$$a x_0 + b y_0 = c = r d x_0 + s d y_0 = (r x_0 + s y_0) d$$

أي أن $d | c$.

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

ولما كان $d = (a, b)$ فيوجد عددان صحيحان m , n بحيث $d = a m + b n$

وبضرب طرفي هذه العلاقة بـ t نجد :

$$t d = a (t m) + b (t n) = c$$

أي يوجد عددان $x_0 = t m$, $y_0 = t n$ يحققان المعادلة : $a x + b y = c$

لنثبت الآن أنه إذا عرفنا الحل الخاص x_0 , y_0 للمعادلة (١) فإن أي حل (x, y) لها يكتب على النحو :

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

لذا نكتب $a x_0 + b y_0 = c = a x + b y$

$$a (x - x_0) = b (y_0 - y) \qquad (٢)$$

ولما كان $d=(a,b)$ فإن ثمة a_0, b_0 بحيث $(a_0, b_0)=1$, $b=b_0 d$

, $a=a_0 d$ نعوض في (٢) فنجد :

$$a_0 (x-x_0) = b_0 (y_0 - y) \qquad (٣)$$

ومنه $a_0 \mid b_0 (y_0 - y)$ ولكن

$(a_0, b_0)=1$ بالتالي $a_0 \mid (y_0 - y)$

أي $y_0 - y = a_0 t \qquad t \in Z$

أو $y = y_0 - a_0 t = y_0 - \frac{a}{d} t$

وبالتعويض في (٣) نجد :

$$a_0 (x - x_0) = b_0 a_0 t \Rightarrow x - x_0 = b_0 t$$

$$x = x_0 + b_0 t = x_0 + \frac{b}{d} t$$ وهو المطلوب

وللمعادلة عدد غير منته من الحلول .

- **ملاحظة (١)** : إذا كان $d-1$ فإن $x = x_0 + bt$ $\quad y = y_0 - at$ هي جميع حلول المعادلة (والمعادلة لها حل دوماً) .

- **ملاحظة (٢)** : إن المبرهنة السابقة مع خوارزمية اقليدس تزودنا بطريقة عملية لإيجاد حلول معادلة ديوفانتس الخطية (١) ومن أجل ذلك نبدأ بتعيين القاسم المشترك الأعظم للعددين a , b ثم كتابة هذا القاسم المشترك الأعظم كتركيب خطي لهما ومن ثم نعين حلول المعادلة (١) .

مثال (١) : عين جميع حلول المعادلة $172 x + 20 y = 1000$ إن وجدت ؟

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

$$172 = 8 \times 20 + 12$$

$$20 = 1 \times 12 + 8$$

$$12 = 1 \times 8 + 4$$

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

تلاحظ أن $4 \mid 1000$ 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

$$y_0 = -4250 \qquad\qquad x_0 = 500$$

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 $x > 0$, $y > 0$ ففي المثال السابق نكتب :

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

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 (٢) : عين حلول المعادلة $6x + 51y = 22$ إن وجدت ؟

نلاحظ أنّ : $(6,51)=3$ ولكن $3 \nmid 22$

وليس للمعادلة أي حل .

مثال (٣) : هل للمعادلة : $7x+9y=5$ حلول ؟ أوجدها في حال الإيجاب

نلاحظ أنّ $d=(7,9)=1$ وللمعادلة حل

نكتب :

$$9=1\times 7+2$$

$$7=3\times 2+1$$

$$2=1\times 2+0$$

$$d=1=7-(2\times 3)$$

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

$$1=7(4)+9(-3)$$

نضرب الطرفين بـــ 5 :

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

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

١-٤-٣ ثلاثيات فيثاغورث (*phytha gorean triple*)

اكتشف البابليون (حوالي2000 ق.م) العلاقة التي تـربط بـين أضـلاع المثلث القائم أي العلاقة $x^2+y^2=z^2$ وعينوا أطوال أضلاع عدد مـن هـذه المثلثات منها $(120,119,169)$, $(4961,6480,8161)$

ولم يعثر على برهان ذلك ولا على شرح لطريقة الوصول إلى هـذه الأرقـام الكبيرة . وقد قدم برهاناً لوجـود حلـول صـحيحة للمعادلـة $x^2+y^2-z^2$ الرياضي اليوناني فيثاغورث حوالي 500 ق. م وهذه المعادلة هي صنف مـن المعادلات ديوفانتس التربيعية . وتسمى الأعداد الـصحيحة (x,y,z) التـي تحقق هذه المعادلة ثلاثيات فيثاغورث ولنبحث في إيجاد حلول هذه المعادلة .

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

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

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

ومنه $p \mid x^2 \wedge p \mid y^2$ ومنه $p \mid x^2 + y^2 = z^2$ وهذا يقتضي : $p \mid z^2$ وهذا يناقض كون $(x, y, z) = 1$ أي أن : $(x, y) = 1$ وبالطريقة ذاتها نثبت أن : $(x, z) = (z, y) = 1$.

- **تمهيدية (٢) :** إذا كان (x, y, z) ثلاثي فيثاغورث وكان $(x, y, z) = d$ 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 $d \mid x,\ d \mid y,\ d \mid z$ 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

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

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

لذلك نكتب :

$$(x_0 d, y_0 d, z_0 d) = ((x_0 d, y_0 d), z_0 d) = (d(x_0, y_0), z_0 d)$$

ومنه :

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

- **ملاحظة :** إذا كان ثلاثي فيثاغورث (x_0, y_0, z_0) أولياً وإذا كان k عدداً صحيحاً أكبر من الصفر فإن $(k x_0, k y_0, k z_0)$ هو ثلاثي فيثاغورث.

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

– **تمهيدية (٣)** : إذا كان ثلاثي فيثاغورث (x, y, z) أولياً فإن أحد العددين x, y 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 $x^2 = 8M_1 + 1$, $y^2 = 8M_2 + 1$ وبالتالي $z^2 = x^3 + y^2 = 8M + 2$ وهذا غير ممكن لأنه لو كان z عدداً فردياً لكان $z^2 = 8n + 1$ ولو كان z عدداً زوجياً لكان $z^2 = 4n^2$.

٨– **تمهيدية (٤)** : إذا كان $a.b = c^n$ حيث $(a, b) = 1$ فإنه يوجد b_1, a_1 بحيث $a = a_1^n$, $b = b_1^n$.

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

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

ولما كان a , b أوليين نسبياً فإن جميع الأوليات $p_i^{\alpha_i}, q_j^{\beta_j}$ مختلفة (فهي أولية نسبياً 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 فـإن 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 ممـا يعني أن $k_1 + k_2 = t$ (عدد العوامل المختلفة في الطرف الأول يساوي عـدد 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

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

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

مبرهنة * : إن جميع الحلول الصحيحة غير الصفرية لمعادلة فيثاغورث $x^2 + y^2 = z^2$ حيث y عدد زوجي و $(x, y, z) = 1$ تعطى بالعلاقات

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

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

---

* لمعرفة إسهامات العرب في هذا الموضوع انظر رسالة الخازن حول المثلثات العددية قائمة الزاوية صفحة ٢٤٢ والقضية (١) صفحة ٢٤٥ من كتاب د. رشدي الراشد (تاريخ الرياضيات العربية بين الجبر والحساب / منشورات مركز دراسات الوحدة العربية .

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

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

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

فإن d سيقسم مجموعهما وفرقهما أي يقسم z, x وهذا غير ممكن لأن $(x, z) = 1$ 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 (٤) أمكننا أن نكتب :

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

ومنه نجد أن :

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

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 (١) 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 (١) : 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 :

$$\begin{cases} r+s=15 \\ r-s=1 \end{cases} \quad \text{أو} \quad \begin{cases} r-s=3 \\ r+s=5 \end{cases}$$

بحل المجموعتين نجد :

$$\begin{cases} r=8 \\ s=7 \end{cases} \quad \text{أو} \quad \begin{cases} r=4 \\ s=1 \end{cases}$$

وثلاثيات فيثاغورث المطلوبة هي :

$$(15, 8, 17) \quad \text{و} \quad (15, 112, 113)$$

مثال (٢) : 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

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

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

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

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

ومنه فإن :

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

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

مثال (٣) : أثبت أن نصف قطر الدائرة الماسة داخلاً لأضلاع مثلث فيثاغورث هو عدد صحيح دائماً .

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

نحسب مساحة المثلث بطريقتين ونكتب :

$$S=\frac{1}{2}xy=\frac{1}{2}R(x+y+z) \qquad (١)$$

نعوض قيم x, y, z التالية :

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

في العلاقة (١) ثم نحسب R فنجد :

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

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

وهو عدد صحيح دائماً .

تمارين

٨- أوجد حلول المعادلات :

$56\ x + 72\ y = 40$

$24\ x + 138\ y = 18$

$221\ x + 91\ y = 117$

$84\ x - 438\ y = 165$

٢- أوجد الحلول الموجبة للمعادلات

$30\ x + 17\ y = 300$

$158\ x - 57\ y = 7$

$54\ x + 21\ y = 906$

$123\ x + 360\ y - 99$

٨- أوجد الحل الكامل للمعادلات

$2\ x + 11\ y = 5$

$18\ x - 21\ y = 15$

$2\ x + 12\ y = 6$

٤- أوجد جميع ثلاثيات فيثاغورث الأولية التي فيها $y=28$.

٥- أثبت أنه إذا كان (x, y, z) ثلاثي فيثاغورث أولي فإن $12 \mid x.y.z$

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

٧- أوجد دستوراً 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

٨- 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 : الجذور الأولية والأدلة

الفصل الأول

التطابقات

- تعريف التطابق
- صفوف البواقي
- مجموعة البواقي التامة
- خواص التطابقات

٢-١ التطابقات (*Congruence*)

إن أول من تعرض لفكرة التطابق ووضع رمزها هو الرياضي الألماني فريدريك غاوس (C . F . Gauss)(1855 – 1777 م) في" كتاب الحساب" .

٢-١-١ تعريف التطابق : ليكن $a, b \in Z$ و $m \in Z^+$ نقول إن العدد a يطابق العدد b بالمقاس m ونكتب $a \equiv b(mod\ m)$ إذا كان $m | a-b$ أو يوجد $M \in Z$ بحيث $a - b = M m$. أما إذا كان $m \nmid a-b$ فإنا نقول إن a لا يطابق b بالمقاس m ونكتب $a \not\equiv b(mod\ m)$.

٢-١-٢ صفوف البواقي :

رأينا أنه إذا كان m عدداً صحيحاً أكبر من الواحد و $n \in Z$ فإنه يوجد عددان وحيدان q, r بحيث يكون $0 \le r < m$, $n = mq + r$

إن الباقي r يمكن أن يأخذ أيا من القيم $r_i = 0,1,2,.....,m-1$

لنضع جميع الأعداد الصحيحة التي باقي قسمتها 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 $r - 0$ هو المجموعة

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

وصف الباقي $r = 1$ هو المجموعة:

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

وهكذا ...

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

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

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

٢-١-٣ مجموعة البواقي التامة :

- **تعريف:** نسمي مجموعة الأعداد الصحيحة A التي عدد عناصرها يساوي m التي 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 $A=\{0,6,-8,8,4\}$ 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 $\{0,1,2,.....,m-1\}$ هي أبسط مجموعات البواقي التامة بالمقاس m ويطلق عليها أحياناً مجموعة البواقي التامة الصغرى (المفضلة) .

- **نتيجة :** من تعريف التطابق ينتج أنه إذا كان $a \equiv b(mod\ m)$ فهذا يعني أن a , b ينتميان إلى صف واحد من صفوف البواقي بالمقاس m في حين $a \not\equiv b(mod\ m)$ 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 :

$$n = mq + r \Rightarrow n - r = mq \Rightarrow m \mid n - r \Rightarrow n \equiv r(mod\ m)$$

٢-١-٤ خواص التطابقات :

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

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

البرهان : إذا كان $a, b, c \in Z$ و $m \in Z^+$ فإن

- $a \equiv a \pmod m$

لأن: $m \mid a - a$

- و $a \equiv b \pmod m \Rightarrow b \equiv a \pmod m$

لأن:

$$m \mid a - b \Rightarrow m \mid b - a$$

- و $a \equiv b \pmod m \wedge b \equiv c \pmod m \Rightarrow a \equiv c \pmod m$

لأن :

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

٢) إذا كان $a \equiv b \pmod m$ و $k \in Z$ فإن $ka \equiv kb \pmod m$

لأن $a - b = Mm$ فإذا ضربنا الطرفين بالعدد k نجد

$$ka - kb = (kM)m$$

٣) إذا كان $c \equiv d \pmod m \wedge a \equiv b \pmod m$

فإن $a \pm c \equiv b \pm d \pmod m$

البرهان : لما كان $a - b = M_1 m$, $c - d = M_2 m$

فإن $(a - b) \pm (c - d) = (M_1 \pm M_2) m$

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

ويمكن تعميم هذه الخاصة فنكتب : إذا كان $a_i \equiv b_i \,(mod\ m)$ من أجل جميع القيم $i = 1, 2, ..., n$ فإن $\sum_{1}^{n} a_i \equiv \sum_{1}^{n} b_i \,(mod\ m)$ ويمكن إثبات ذلك بطريقة الاستقراء الرياضي .

٤) مبرهنة: إذا كان

$a \equiv b (mod\ m)$ و $c \equiv d (mod\ m)$ فإن $a\,c \equiv b\,d (mod\ m)$

البرهان : لدينا $a = b (mod\ m) \Rightarrow \quad a\,c \equiv b\,c (mod\ m)$

و $c \equiv d (mod\ m) \Rightarrow \quad b\,c \equiv b\,d (mod\ m)$

أي $a\,c \equiv b\,d (mod\ m)$ وهو المطلوب .

٥) إذا كان $a \equiv b \,(mod\ m)$ فإن $a^n \equiv b^n \,(mod\ m)$ 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 :

$$a^k \equiv b^k \,(mod\ m)$$

وحسب الخاصة (٤) نكتب :

$$a \,.\, a^k \equiv b \,.\, b^k \,(mod\ m)$$

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

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

٦) إذا كان $a \equiv b \,(mod\ m)$ وإذا كان $f(x) = \sum_{i=0}^{n} a_i x^i$ حيث $a_i \in Z$ $0 \leq i \leq n$ فإن :

$$f(a) \equiv f(b) \,(mod\ m)$$

البرهان :

بما أن $a \equiv b \pmod m$ فإن $a^i \equiv b^i \pmod m$ حسب الخاصة (٥)

وكذا $a_i a^i \equiv a_i b^i \pmod m$ أي $\sum_{i=0}^{n} a_i a^i \equiv \sum_{i=0}^{n} a_i b^i \pmod m$

أي $f(a) \equiv f(b) \pmod m$.

مثال : لدينا $2 \equiv -4 \pmod 6$ فإذا كان $f(x) = x^2 - x + 5$ فإن :

$f(2) - 7 \quad , \quad f(-4) - 25 \quad , \quad 7 \equiv 25 \pmod 6 \Leftrightarrow f(2) \equiv f(-4) \pmod 6$

٧) **مبرهنة :** إذا كان $ka \equiv kb \pmod m$ وإذا كان $d = (k, m)$ فإن

$$a = b \left(\bmod \frac{m}{d}\right)$$

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

$$k = k_0 d \ , \ m = m_0 d$$

و $(k_0, m_0) = 1$ وبما أن $ka \equiv k\,b \pmod m$ فإن

$$k_0\, d(a-b) = M\, m_0 d \quad \Leftarrow \quad k(a-b) = M\, m$$

ومنه $k_0\,(a-b) = M\, m_0$ أي أن $m_0 \mid k_0\,(a-b)$ ولما كان

$(k_0, m_0) = 1$ ينتج أن :

$m_0 \mid a - b$ أي $a \equiv b \pmod{m_0}$ حيث $m_0 = \dfrac{m}{d}$

- **نتيجة (١) :** ينتج من الخاصة السابقة أنه إذا كان $ka \equiv k\,b \pmod m$ وكان $(k, m) = 1$ فإن $a \equiv b \pmod m$ أي يمكن اختصار العامل المشترك بين طرفي تطابق إذا كان هذا العامل أولياً نسبياً مع المقاس .

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

في حـــين $77 \equiv -28 \ (mod\ 15)$ ومنه نجد $11 \equiv -4 \ (mod\ 15)$

لأن :

$$(77,-28) = 7 \text{ و } (7,15) = 1$$

- **نتيجة (٢) :** إذا كان $ca \equiv cb \ (mod\ p)$ حيث p عدد أولي لا يقسم c فإن $a \equiv b \ (mod\ p)$ وذلك لأن $(a,p) = 1$ في هذه الحالة

- **ملاحظة (١) :** إذا كان العامل المشترك $k \equiv 0 \ (mod\ m)$ فإن $(k,m) = m$ والاختصار يؤدي إلـــى النتيجـــة $a \equiv b \ (mod\ 1)$ وهـــي علاقة صحيحة مهما تكن الأعداد b, a .

- **ملاحظة (٢) :** إذا كان $a\,b \equiv a.0 \ (mod\ m)$ و $(a,m) = 1$ فإن المبرهنة السابقة تعطي $b \equiv 0 \ (mod\ m)$.

وإذا كان $a\,b \equiv a.0 \ (mod\ p)$ حيث p عدد أولي فإما أن يكون $a \equiv 0 \ (mod\ p)$ أو $b \equiv 0 \ (mod\ p)$.

٨) إذا كان $a \equiv b \ (mod\ m)$ وكان $n \mid m$ فإن $a \equiv b \ (mod\ n)$.

البرهان : لدينا $m \mid a-b$ و $n \mid m \Rightarrow n \mid a-b$

ومنه $a \equiv b \ (mod\ n)$

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

وإذا $a \equiv b \ (mod\ m_i)$ فإن $a \equiv b \ (mod\ m)$ حيث

$$m = lcm\ (m_1, m_2, ..., m_k)$$

البرهان : لدينا $m_i \mid a-b$ ولما كان $m_i \mid m$ من أجل $1 \le i \le k$ فإن $a - b$ مضاعف مشترك للأعداد m_i فهو مضاعف للمضاعف المشترك الأصغر m أي $m \mid a-b$ و $a \equiv b \ (mod\ m)$.

- **نتيجة** : إذا كانت m_i أولية نسبياً مثنى مثنى فإنها أولية نسبياً

و $m = m_1.m_2.....m_k$ فإذا كان $a \equiv b\ (mod\ m_i)$ من أجل

$i = 1,2,...,k$ فإن $a \equiv b\ (mod\ m_1.m_2.....m_k)$.

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

$a \equiv b\ (mod\ p_i^{\alpha_i}) \Leftarrow a \equiv b\ (mod\ m)$ حيث $i = 1,2,...,k$

١٠) **مبرهنة** : إذا كان $a \equiv b\ (mod\ p^r)$ حيث $a\ ,\ b\ ,\ r$ أعداداً صحيحةً

و $r \geq 1$ و p عدداً أولياً ، 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 الإستقراء : لنفترض أن العلاقة صحيحة من أجل $s = k \geq 0$

ولنثبت صحتها من أجل $s = k+1$ فنكتب :

$$a^{p^k} \equiv b^{p^k}\ (mod\ p^{r+k}) \Rightarrow a^{p^k} = b^{p^k} + M\ p^{r+k}$$

نرفع الطرفين إلى القوة p فنجد :

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

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

ولما كانت قوى p بدءاً من الحد الثاني هي $r+k+1$ ، $2r+2k+1$ .....

وكلها $r+k+1 \leq$ فإن جميع الحدود بدءاً من الحد الثاني 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 $s \geq 0$.

تمرين(١) : 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 :

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

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

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

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

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

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

تمرين(٢) : من أجل $n \in Z^+$ أثبت أن $15 \mid 2^{4n} - 1$

الحل: لدينا

$$2^4 \equiv 16 \equiv 1 (\ mod 15) \Rightarrow (2^4)^n \equiv 1 (\ mod\ 15)$$

أي: $15 \mid 2^{4n} - 1$

تمرين(٣) : من أجل $n \geq 0$ أثبت أن $8 \mid 3^{2n} + 7$

الحل: إن

$$3^2 \equiv 9 \equiv 1 (\ mod\ 8) \Rightarrow 3^{2n} \equiv 1 (\ mod\ 8) \ \Rightarrow \ 3^{2n} + 7 \equiv 1 + 7 (\ mod\ 8)$$

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

تمرين(٤) : أوجد أصغر عدد صحيح موجب k يحقق العلاقة :

$$31 \mid 33(26)^2 - k$$

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

$$33(26)^2 \equiv k(\ mod\ 31)$$

ولما كان $33 \equiv 2\ (\ mod\ 31)$ و $26 \equiv -5(\ mod\ 31)$

فإن $(26)^2 \equiv 25(\ mod\ 31)$

أي أن $33(26)^2 \equiv 50(\ mod\ 31)$

وأخيراً $33(26)^2 \equiv 19(\ mod\ 31)$ و $k = 19$

تمرين (٥) : أوجد باقي قسمة $\sum_{1}^{1000} k!$ على 24

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

$$\sum_{1}^{1000} k! = 1 + 2 + 6 \equiv 9(\ mod\ 24)$$

وباقي القسمة هو 9 .

الفصل الثاني

التطابقات الخطية

- التطابق الخطي
- الكسور البسيطة المستمرة المنتهية
- النظير الضربي
- مبرهنة الباقي الصينية
- مبرهنة فيرما الصغرى
- مبرهنة ويلسون وعكسها

٢-٢ التطابقات الخطية *Linear congruences*

٢-٢-١ تعريف : التطابق الخطي هو معادلة من الشكل :

$$a\,x \equiv b(\ mod\ m) \qquad (١)$$

حيث $a\ ,\ b$ أعداد صحيحة معلومة x عدد صحيح مجهول وm عدد صحيح أكبر من الواحد وحل التطابق الخطي هو إيجاد قيمة العدد الصحيح x_0 الذي يحقق المعادلة

$$a\,x_0 \equiv b(\ mod\ m)$$

ومن تعريف التطابق نعلم أن هذا التطابق يتحقق إذا وفقط إذا كان $m \mid a\,x_0 - b$ أي إذا وفقط إذا وجد عدد y_0 بحيث $a\,x_0 - b = m\,y_0$ أي أن مسألة حل تطابق خطي تؤول إلى مسألة إيجاد الحلول الكاملة لمعادلة ديوفانتس الخطية $a\,x - m\,y = b$.

- **ملاحظة :** نعد الحلول المتطابقة بالمقاس m للتطابق الخطي حلاً واحداً

فعلى سبيل المثال : إن $x = 3$ و $x = -9$ كل منهما يحقق التطابق $3\,x \equiv 9(\ mod\ 12)$ لذا نعدهما حلاً واحداً ونعني بعدد حلول تطابق عدد الحلول غير المتطابقة بالمقاس m .

٢-٢-٢ مبرهنة : يكون للتطابق الخطي $a\,x \equiv b(\ mod\ m)$ حلاً إذا وفقط إذا كان $d \mid b$ حيث $d = g\,c\,d\ (a, m)$ ، وإذا كان $d \mid b$ 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 $d \mid b$ كما أثبتنا أنه إن كان x_0, y_0 هو حل خاص لمعادلة ديوفانتس فإن الحل الكامل لها هو : $t \in Z$

$$x = x_0 + \frac{m}{d}t \qquad y = y_0 - \frac{m}{d}t$$

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

أي لنكتب :

$$x_0 \ , \ x_0 + \frac{m}{d} \ , \ x_0 + \frac{2m}{d} \ , ..., x_0 + \frac{(d-1)}{d} m$$

ولنثبت أن هذه الحلول كلها غير متطابقة بالمقاس m إذ لو تطابق حلان موافقان للقيمتين t_2 , t_1 لأمكن أن نكتب :

$$x_0 + \frac{m}{d} t_1 \equiv x_0 + \frac{m}{d} t_2 \ (mod \ m) \qquad 0 \le t_1 < t_2 \le d-1$$

ومنه

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

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 $t = 0,1,2,....,d-1$ 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 التي عددها يساوي d .

في الحقيقة بما أن $t \ge d$ فهي تكتب على النحو $t = qd + r$ حيث $0 \le r < d$ أي $0 \le r \le d-1$ ، 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 (١) : أوجد حلول التطابق $6x\equiv 2(\ mod\ 9)$

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

تمرين (٢) : أوجد حلول التطابق $9x\equiv 21(\ mod 30)$

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 $x\equiv x_0+10\,t$ حيث $t=0,1,2$

و $x_0=9$

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 :

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

أي الحلول غير المتطابقة بالمقاس 30 هي :

$x \equiv -1 \pmod{30}$ و $x \equiv -11 \pmod{30}$ و $x \equiv -21 \pmod{30}$

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

٢-٢-٣ 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 :

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

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

ويرمز :

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

مثال (١) :

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

مثال (٢) :

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

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

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 :

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

ففي المثال (٢) يمكن أن نكتب :

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

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

٢-٢-٤ مبرهنة : إذا كان لدينا الكسر المستمر المنتهي $< a_1, a_2, ..., a_n >$ وأدخلنا الرموز التالية :

$$q_1 = 1 \quad , \quad p_1 = a_1$$

$$q_2 = a_2 \quad , \quad p_2 = a_1 a_2 + 1$$

$$q_3 = a_3\ q_2 + q_1 \quad , \quad p_3 = a_3\ p_2 + p_1$$

$$\ldots\ldots \qquad \ldots\ldots$$

$$q_i = a_i\ q_{i-1} + q_{i-2} \quad , \quad p_i = a_i\ p_{i-1} + p_{i-2}$$

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 :

١- 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 .

٢- 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 :

$$c_k = \frac{a_k p_{k-1} + p_{k-2}}{a_k q_{k-1} + q_{k-2}} = a_1 + \cfrac{1}{a_2 + \cfrac{1}{a_3 + \cfrac{\ }{\cdots\cdots + a_k}}}$$

و

$$c_{k+1} = a_1 + \cfrac{1}{a_2 + \cfrac{1}{a_3 + \cfrac{\quad}{\cdots\cdots\cdots\cdots + a_k + \cfrac{1}{a_{k+1}}}}}$$

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

$$c_{k+1} = \frac{(a_k + \frac{1}{a_{k+1}})\, p_{k-1} + p_{k-2}}{(a_k + \frac{1}{a_{k+1}})\, q_{k-1} + q_{k-2}} = \frac{\{(a_k \cdot a_{k+1} + 1)\, p_{k-1} + a_{k+1}\, p_{k-2}\} / a_{k+1}}{\{(a_k \cdot a_{k+1} + 1)\, q_{k-1} + a_{k+1}\, q_{k-2}\} / a_{k+1}} =$$

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

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

٢-٢-٥ 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 :

$$q_1 = 1 \quad , \quad q_2 = a_2 \quad , \quad p_1 = a_1 \quad , \quad p_2 = a_2 a_1 + 1$$

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

$$p_2\, q_1 - p_1\, q_2 = (a_2 a_1 + 1)(1) - a_1\, a_2 = 1 = (-1)^2$$

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

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

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 : $d \mid p_n \wedge d \mid q_n$

فإن $d \mid p_n\, q_{n-1} - p_{n-1}\, q_n$ أي $d \mid 1$ وبالتالي $d = 1$

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

تمرين (١): لنوجد حل التطابق $79\,x \equiv 3 \pmod{103}$ بطريقة الكسور المستمرة .

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

$$79\,x + 103\,y = 3$$

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

$$\frac{79}{103} = 0 + \cfrac{1}{1 + \cfrac{24}{79}}$$

$$= 0+\cfrac{1}{1+\cfrac{1}{3+\cfrac{7}{24}}} = 0+\cfrac{1}{1+\cfrac{1}{3+\cfrac{1}{\frac{24}{7}}}} =$$

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

أي أن

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

و

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

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

$$c_1 = \frac{p_1}{q_1} = 0 \qquad c_2 = \frac{p_2}{q_2} = 1$$

$$c_3 = \frac{a_3 p_2 + p_1}{a_3 q_2 + q_1} = \frac{3}{4} = \frac{p_3}{q_3} \qquad c_4 = \frac{a_4 p_3 + p_2}{a_4 q_3 + q_2} = \frac{10}{13} = \frac{p_4}{q_4}$$

$$c_5 = \frac{a_5 p_4 + p_3}{a_5 q_4 + q_3} = \frac{23}{30} = \frac{p_5}{q_5} \qquad c_6 = \frac{a_6 p_5 + p_4}{a_6 q_5 + q_4} = \frac{79}{103} = \frac{p_6}{q_6}$$

نطبق المبرهنة الثانية فنجد :

$$p_6 q_5 - p_5 q_6 = 79 \times 30 - 103 \times 23 = 1$$

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

والحل الكامل للتطابق : $\Rightarrow \quad x=x_0+103\;t=90+103\,t$

أي : $x\equiv 90\ (\,mod\ 103)$

تمرين (٢) : لنوجد حل التطابق :

$$187\ x\equiv 2\ (\,mod\ 503)$$

نوجد الكسر البسيط المستمر للكسر $\frac{187}{503}$ فنجد :

$$\frac{187}{503}=<0,2,1,2,4,2,6>$$

نوجد التقريبات المتتالية :

$$c_1=\frac{0}{1}=0 \qquad c_2=\frac{1}{2} \qquad c_3=\frac{1}{3} \qquad c_4=\frac{3}{8}$$

$$c_5=\frac{13}{35}=\frac{p_5}{q_5} \qquad c_6=\frac{29}{78}=\frac{p_6}{q_6} \qquad c_7=\frac{187}{503}=\frac{p_7}{q_7}$$

وبالتالي

$$p_7\,q_6-p_6\,q_7=(-1)^7 \;\Rightarrow 187\,(78)-\ 503\,(29)=-1$$

أي $187\,(-156)+503(58)=2$

والحل المطلوب هو :

$$x\equiv -156\ (\,mod\ 503)\ \equiv\ 347\ (\,mod\ 503)$$

٢-٢-٦ النظير الضربي

تعريف : نقول إن a^* هو النظير الضربي للعدد الصحيح a بالمقاس m إذا كان $a.a^*\equiv 1\ (\,mod\ m)$

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 $2x \equiv 1 \pmod 4$ ليس له حل لأن $(2,4)=2$ و $2 \nmid 1$

وبشكل عام لا يوجد نظير ضربي لأي عدد زوجي إذا كان المقاس زوجياً .

٢-٢-٧ 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 $a\,x \equiv 1 \pmod m$ حل هو أن يكون d القاسم المشترك الأعظم للعددين m , a قاسما للواحد وهذا لا يصح إلا عندما $d=1$ أي $(a,m)=1$.

تمرين (١) : عين النظير الضربي للعدد 17 بالمقاس 25 :

الحل : لنوجد حل التطابق $17\,x \equiv 1 \mod 25$ فنجد

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

والعدد 3 هو النظير الضربي المطلوب .

تمرين (٢) : أوجد النظير الضربي للعدد 71 بالمقاس 55 :

الحل : لنوجد حل التطابق $71\,x \equiv 1 \pmod{55}$ بطريقة الكسور البسيطة المستمرة فنكتب :

$$\frac{71}{55} = 1 + \cfrac{1}{3 + \cfrac{1}{2 + \cfrac{1}{3 + \cfrac{1}{2}}}} = \langle 1,3,2,3,2 \rangle$$

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 الضربي للعدد 71 بالمقاس 55 هو -24 أي :

$$71^{*} \equiv -24 \ (mod\ 55)$$

٢ – ٢–٨ حل جملة تطابقات خطية :

نكتب جملة التطابقات الخطية على النحو : $b_i\, x \equiv a_i \ (mod\ m_i)$

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

ونلاحظ ما يلي :

١– إذا لم يكن لأحد التطابقات ، حل فليس لجملة التطابقات حل .

٢– إذا كان لكل من التطابقات حل فليس بالضرورة أن يكون لجملة التطابقات حل مشترك .

على سبيل المثال :

إن لكلٍ من التطابقين $3x \equiv 2 \ (mod\, 4)$ و $9x \equiv 3 \ (mod\, 12)$ حل ، ونلاحظ أن $x \equiv 2 \ (mod\, 4)$ يحقق التطابق الأول ولا يحقق التطابق الثاني كما أن $x \equiv 3 \ (mod\, 4)$ يحقق التطابق الثاني $3x \equiv 1 \ (mod\, 4)$ ولا يحقق التطابق الأول وليس للتطابقين حل مشترك .

٢ – ٢–٩ 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 ١٠٠ 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 :

$$x \equiv a_1 \ (mod\, m_1)$$
$$x \equiv a_2 \ (mod\, m_2)$$
$$\ldots\ldots\ldots\ldots$$
$$x \equiv a_k \ (mod\, m_k)$$

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

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

إن $(M_i, m_i) = 1$ لذا يوجد للتطابق $M_i m_i' \equiv 1 \ (mod\, m_i)$ حل من أجل $i = 1, 2, \ldots\ldots, k$. أي يوجد للعدد M_i نظير ضربي بالمقاس m_i نسميه m_i' .

لنكتب العدد x على النحو :

$$x = m_1' M_1 a_1 + m_2' M_2 a_2 + \ldots\ldots + m_k' M_k a_k$$

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

$$x = m_i' M_i a_i \equiv a_i \ (mod\, m_i) \qquad 1 \le i \le k$$

و x 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 :

$m_i \mid x - x'$ ولما كان m هو المضاعف المشترك الأصغر للأعداد m_i فإن $m \mid x - x'$ و $x = x' \ (mod\, m)$.

مثال (١) : 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 بينهـا مثنـى مثنـى ولجملـة 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 .

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

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

والحل المشترك لجملة التطابقات هو :

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

مثال (٢) : أوجد حل التطابق $19\ x \equiv 1 \ (mod 140)$ باستخدام مبرهنة الباقي الصينية :

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

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

والمقاسات 4 , 5 , 7 أولية نسبياً مثنى مثنى ولهذه الجملة حـل لإيجـاده نكتب :

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

وحلول التطابقات :

$$35\, m_1' \equiv 1 (mod\, 4) \quad \Rightarrow \quad m_1' = -1$$
$$28\, m_2' \equiv 1 (mod\, 5) \quad \Rightarrow \quad m_2' = 2$$
$$20\, m_3' \equiv 1 (mod\, 140) \quad \Rightarrow \quad m_3' = -1$$

والحل المشترك :

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

وهو حل التطابق المطلوب .

مثال (٣) : المطلوب إيجاد الحل المشترك لجملة التطابقات التالية :

$$x \equiv 10 (mod\, 24)$$
$$x \equiv 50 (mod\, 88)$$
$$x \equiv 28 (mod\, 99)$$

الحل :

نلاحظ أن المقاسات غير أولية نسبياً مثنى ونلاحظ أن :

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

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

إن حل التطابق الأول يكافىء حل جملة التطابقين $x \equiv 10 (mod\, 3)$ (1)

$x = 10 (mod\, 8)$ (2)

كما أن حل التطابق الثاني يكافىء حل جملة التطابقين $x \equiv 50 (mod\, 8)$ (3)

$x \equiv 50 (mod\, 11)$ (4)

و حل التطابق الثالث يكافىء حل جملة التطابقين $x \equiv 28 (mod\, 9)$ (5)

$x \equiv 28 (mod\, 11)$ (6)

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

أن $2 \equiv 10 \equiv 50 (mod\, 8)$ أي أن التطابق (2) هو ذات التطابق (3)

وأن $6 \equiv 50 \equiv 28 (mod 11)$ أي أن التطابق (4) هو ذات التطابق (6)
كما نلاحظ أن $1 \equiv 10 \equiv 28 (mod 9)$. وكل حل للتطابق (5) يحقق التطابق (1) لأن $3 \mid 9$ أي أن إيجاد حل جملة التطابقات المعطاة يؤول إلى إيجاد حل

جملة التطابقات الثلاث :

$$x \equiv 2 (mod 8)$$
$$x \equiv 6 (mod 11)$$
$$x \equiv 1 (mod 9)$$

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 $m_1' \equiv 3 (mod 8) \quad m_2' \equiv 2 (mod 11) \quad m_3' \equiv 4 (mod 9)$

والحل المشترك المطلوب :

$$x \equiv (3)(99)(2) + (2)(72)(6) + (4)(88)(1) \equiv 1810 \ (mod\ 792)$$
$$x \equiv 226 \ (mod\ 792)$$

وأخيراً سنورد المبرهنة التالية دون برهان

مبرهنة : يوجد لجملة التطابقات :

$$x \equiv a_1 \ (mod\ m_1)$$
$$x \equiv a_2 \ (mod\ m_2)$$
$$\dots\dots\dots\dots$$
$$x \equiv a_k \ (mod\ m_k)$$

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

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

وتسمى جملة التطابقات التي تحقق الشرط : $a_i \equiv a_j \,(mod\ d_{ij})$ جملة منسجمة (*compatible system*) .

٢-٢-١٠ مبرهنة فيرما الصغرى : « *Fermat's theorem* »

لقد وضع فيرما (1601-1665) « *Pierre de Fermat* ».هـذه المبرهنـة عام 1640 وأول إثبات لها تم من قبل أولر بعد مئة عام .

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

البرهان : لنكتب مضاعفات العدد الصحيح a التالية :

$$A = \{1a\ ,\ 2a\ ,3a\ ,....,\ (p-1)\ a\}$$

نلاحظ أن هذه الأعداد غير متطابقة فيما بينها بالمقاس p ، إذ لو كان :

$$r\,a \equiv s\,a\ (\ mod\ p) \qquad 1 \le r < s \le p-1$$

لاستطعنا اختصار a لأن $(a, p) = 1$ مما يؤدي إلى العلاقة $r \equiv s\ (\ mod\ p)$ وهذا مستحيل ، كما أن عناصر المجموعة A أولية نسبياً مع p لذا فإن كـل عنصر من عناصر المجموعة A يطابق بالمقاس p عنصراً واحداً من عناصر المجموعة : $A = \{1\ ,\ 2\ ,3\ ,....,\ p-1\}$ مما يدل على أن جداء عناصـر A يساوي جداء عناصر المجموعة A بالمقاس p الأمر الذي يعطي :

$$a\ .\ 2a\ .3a\ .....\ (p-1)\ a \equiv 1\ .\ 2\ .3\ .....\ (p-1)\ (mod\ p)$$

ولما كان العدد الأولي p لا يقسم أياً من الأعداد $1, 2, ..., (p-1)$ فهـو لا يقسم جداءها لذا يمكن اختصار $(p-1)!$ من الطرفين لنحصل على :

$$a^{p-1} \equiv 1 (mod\ p)$$

- نتيجة (١) : يمكن صياغة المبرهنة السابقة كما يلي :

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

الإثبات : إذا كـــان $p \nmid a$ فـــإن $(p,a)=1$ و $a^{p-1} \equiv 1 (mod\ p)$ نـــضرب الطرفين بـــ a لنحصل على المراد :

$a^p \equiv a\ (mod\ p)$ والعلاقة صحيحة .

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

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

تمرين : أثبت أن : $5^{38} \equiv 4\ (mod 11)$

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

ولدينا : $5^2 \equiv 25 \equiv 3\ (mod 11)$ و $5^{10} \equiv 1\ (mod 11)$ ومنه

$$5^{38} \equiv (1)^3 (3)^4 \equiv 81\ (mod 11) \equiv 4\ (mod 11)$$

– **نتيجة (٢) :** إذا كان q, p عددين أوليين مختلفين وكان :

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

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

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

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

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

$p \mid a^{pq} - a$ و $p \mid a^{pq} - a$ و $(p,q) = 1$ ومنه ينتج أن

$pq \mid a^{pq} - a$ أي $a^{pq} \equiv a\ (mod\ pq)$

تمرين : أثبت أن $2^{340} \equiv 1\ (mod\ 341)$

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

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

وحسب خواص التطابقات نجد:

$$2^{31} \equiv 2^{30} . 2 \equiv (2^{10})^3 . 2 \equiv 2\ (mod\ 11)$$

ومن جهة أخرى لدينا : $2^{10} \equiv (2^5)^2 \equiv (1)^2 \ (mod\ 31)$

أي أن : $2^{11} \equiv 2 \ (mod\ 31)$

فحسب النتيجة (٢) السابقة نجد أن :

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

طريقة ثانية : كتبنا حسب فيرما $2^{10} \equiv 1 \ (mod\ 11)$ ويمكن أن نكتب

$$2^{340} \equiv (2^{10})^{34} \equiv 1 \ (mod\ 11) \quad \Rightarrow \quad 11 \mid 2^{340} - 1$$

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

وحسب خواص التطابقات نكتب :

$$2^{340} \equiv (2^{30})^{11} \ . \ 2^{10} \equiv 1 \ (mod\ 31) \quad \Rightarrow \quad 31 \mid 2^{340} - 1$$

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

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

– **تعريف :** تسمى الأعداد الصحيحة غير الأولية n التي تحقق العلاقة $2^n \equiv 2 \ (mod\ n)$ أشباه الأوليات (*Pseudoprimes*) .

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

تمرين (١) : إذا كان $(a,35) = 1$ أثبت أن $a^{12} \equiv 1 \ (mod 35)$

الحل : لدينا

$35 = (5)(7)$ و $(a,35) = 1$ ومنه نجد : $(a,7) = 1$ و $(a,5) = 1$

نطبق مبرهنة فيرما فنجد $a^6 \equiv 1 \ (mod 7)$ ومنه ينتج $a^{12} \equiv 1 \ (mod 7)$

أي $7 \mid a^{12}-1$ ومن جهة أخرى :

$$5 \mid a^{12}-1 \Leftarrow a^{12} \equiv 1 \pmod 5 \Leftarrow a^4 \equiv 1 \pmod 5$$

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

تمرين (٢) : إذا كان $(a\,.\,b,42)=1$ أثبت أن $a^6-b^6 \equiv 0 \pmod{168}$

الحل : لدينا

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

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

$$a^6 \equiv 1 \pmod 7\,,\,b^6 \equiv 1 \pmod 7\,,\,a^2 \equiv 1 \pmod 3 \Rightarrow a^6 \equiv 1 \pmod 3$$

و $b^2 \equiv 1 \pmod 3 \rightarrow b^6 \equiv 1 \pmod 3$ ولما كان a , b فرديان لأن $(a.b,8)=1$ يمكن أن تكتب $a^2 \equiv 1 \pmod 8$, $b^2 \equiv 1 \pmod 8$ (برر ذلك)ومنه

$a^6 \equiv 1 \pmod 8$, $b^6 \equiv 1 \pmod 8$. أي أن كل من 7 , 8 , 3 يقسم a^6-b^6 ولما كان $(3\,,7,8)=1$ ينتج $168 \mid a^6-b^6$.

٢-٢-١١ مبرهنة ويلسون- ابن الهيثم أو ما تعرف باسم :(Wilson's theorem)

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

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

إذا كان $p=3$ فإن $3 \mid 2+1$ والعلاقة محققة .

لنثبت صحة العلاقة من أجل $P>3$

ليكن العدد a هو أحد عناصر المجموعة $A=\{2\,,3,.....,(p-2)\}$ ، من الواضح أن $(a,p)=1$ أي أن لكل عنصر a نظير ضربي واحد بالمقاس p يحقق العلاقة : $a\,a^* \equiv 1 \pmod p$ وينتمي إلى مجموعة البواقي التامة للعدد p : $A=\{0,1\,,2,.....,(p-1)\}$.

ولكن من الواضح أن $a^* \not\equiv 0 \ (mod\ p)$. كما أن $a^* \not\equiv \pm 1 \ (mod\ p)$ لأنه لو كان $a^* \equiv \pm 1 \ (mod\ p)$ لنتج أن $a \equiv \pm 1 \ (mod\ p)$ وهذا غير ممكن لأن $a \in A$ وكلا العددين 1 و $-1 \equiv p-1 \ (mod\ p)$ لا ينتميان إلى A ، مما يبين أن a^* ينتمي إلى المجموعة A . ومن جهة أخرى فإن $a \not\equiv a^* \ (mod\ p)$ لأن هذا يقتضي أن يكون $a.a^* \equiv a^2 \equiv 1 \ (mod\ p)$ الأمر الذي يقود إلى العلاقة $a^2 - 1 \equiv (a-1)(a+1) \equiv 0 \ (mod\ p)$ التي تعطي $a \equiv \pm 1 \ (mod\ p)$ 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 بـــ $\frac{p-3}{2}$ زوجاً ، جداء كل ثنائي منها يطابق الواحد بالمقاس p أي أن :

$$2 . 3 .....(p-2) \equiv 1 (\ mod\ p)$$

وبضرب طرفي التطابق بـــ p -1 نجد :

$$1 . 2 . 3.....(p-2)(p-1) \equiv (p-1)! \equiv (p-1)(\ mod\ p)$$

أي

$$(p-1)! \equiv -1 \ (mod\ p)$$

٢ - ٢ - ١٢ عكس مبرهنة ويلسون - ابن الهيثم :

إذا كان $n \geq 2$ و $(n-1)! \equiv -1 \ (mod\ n)$ 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 $d \mid (n-1)!$ (١)

ومن جهة أخرى فإن $d \mid n$ و $n \mid (n-1)! + 1$ $\Leftarrow$

$d \mid (n-1)! + 1$ (٢) ومن العلاقتين (١) و(٢) ينتج أن $d \mid 1$ أي $d = 1$ مما يدل على أن n عدد أولي .

- **ملاحظة :** يمكن صياغة مبرهنة ويلسون- ابن الهيثم وعكسها معاً على النحو :

يكون العدد الصحيح $n > 1$ أولياً إذا كان $(n-1)! \equiv -1 \ (mod\, n)$.

ولكن هذا المعيار للأعداد الأولية معيار نظري بسبب

سرعة تزايد $(n-1)!$ عندما يكون n كبيراً .

تمرين (١) : أثبت أن $18! \equiv -1 (\ mod\ 437)$.

الحل : لدينا $437 = 19 \times 23$ وحسب مبرهنة ويلسون نكتب :

$$18! \equiv -1 \ mod\ (19) \quad , \quad 22! = -1 (mod\, 23)$$

ولكن $22! = 18!(19)(20)(21)(22)$

أي : $22! \equiv 18!(-4)(-3)(-2)(-1)(mod\, 23)$

إذن $22! \equiv 18! \equiv -1 \ (mod\ 23)$

مما سبق يمكن أن نكتب : $19 \mid 18! + 1$ و $23 \mid 18! + 1$

و $(19,23) = 1 \quad \Leftarrow \quad (23)(19) = 437 \mid 18! + 1$

تمرين (٢) : أثبت أن العدد 127 يقسم $7(125!) + 5!$

الحل : بما أن 127 عدد أولي فحسب ويلسون نكتب $126! \equiv -1 \ (mod\ 127)$.

ولدينا

$(126)! \equiv 125!$ 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 (٣) : لنوضح مبرهنة ويلسون بالمثال التالي : ليكن $p = 13$ ولنعرف المجموعة $A = \{2, 3, 4, ..., 11\}$ ولنرتب عناصر A وفق ثنائيات عددها $\frac{13-3}{2} = 5$ فنجد :

$(2)(7) \equiv 1 \ (mod\ 13)$ ، $(3)(9) \equiv 1 \ (mod\ 13)$ ، $(4)(10) \equiv 1 \ (mod\ 13)$

$$(5)(8) \equiv 1 \ (mod\ 13) \quad ، \quad (6)(11) \equiv 1 \ (mod\ 13)$$

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 :**

١. يمكن التعبير عن مبرهنة ويلسون أيضاً كما يلي :

$$(p-1)! \equiv p-1 \ (mod\ p) \quad \text{أو} \quad (p-2)! \equiv 1 \ (mod\ p)$$

حيث p عدد أولي .

٢. نص ابن الهيثم لهذه المبرهنة كما ورد في الملحق (٢) في الأسطر الأربعة الأولى من الصفحة الأخيرة من مخطوطة ابن الهيثم و

... كل عدد أول ... إذا ضربت الأعداد التي قبله بعضها في بعض على الوجه الذي قدمنا وزيد على ما يجتمع واحد كان الذي يجتمع إذا قسم على كل واحد من الأعداد التي قبل العدد الأول بقي منه واحد وإذا قسم على العدد الأول لم يبق منه شيء .

تمارين

١- أعط مثالاً يبين أنه إذا كان $a^2 \equiv b^2 \ (mod\, n)$ فليس من الضروري أن يكون $a \equiv b \ (mod\, n)$.

٢- أعط مثالاً يبين أنه إذا كان $a^k \equiv b^k \ (mod\, n)$ و $k \equiv j \ (mod\, n)$ فليس من الضروري أن يكون $a^j \equiv b^j \ (mod\, n)$.

٣- 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 $c \in Z$.

٤- أثبت بطريقة الاستقراء أنه إذا كان a عدداً صحيحاً فردياً فإن

$$a^{2^n} \equiv 1 \ (\ mod\, 2^{\,n+2}\ )$$

٥- إذا كان n عدداً صحيحاً فردياً لا يقبل القسمة على 3 فبرهن أن

$$72 \ \Big| \ 5n^6 + 3n^4 - 3n^2 - 5$$

٦- أثبت أنه إذا كان العدد الصحيح a لا يقبل القسمة على أي من الأعداد : $2 , 3 , 5 , 7$ كان : $840 \ \Big| \ a^{12} - 1$.

٧- إذا كان $(a,35)=1$ أثبت أن $n^{12} \equiv (mod 35)$.

٨- أثبت أنه إذا كان k عدداً صحيحاً فردياً و $(k,3)=1$

فإن $k^2 \equiv 1 (mod\, 24)$

٩- أوجد باقي قسمة الأعداد 2^{50} و 41^{65} على العدد 7

١٠- أوجد باقي قسمة المجموع $1^5 + 2^5 + 3^5 + \ldots\ldots + 99^5 + 100^5$ على العدد 4 .

١١- إذا كان $(n,30)=1$ أثبت أن 240 يقسم $n^4 + 239$.

١٢- إذا كان $(n,42)=1$ أثبت أن 504 يقسم n^6-1 .

١٣- أثبت أن باقي قسمة $255!$ على العدد الأولي 257 يساوي 1 .

١٤- أوجد الكسور البسيطة المستمرة من أجل كل من الكسور التالية :

$$\frac{119}{32} \quad , \quad \frac{118}{303} \quad , \quad -\frac{503}{187} \quad , \quad -\frac{125}{198}$$

١٥- أوجد الكسر المقابل لـ $<3,1,1,4,1,3>$

١٦- أوجد الحل الكامل لكل من :

$$18\,x \equiv 30\ (mod\ 42) \quad ، \quad 187\,x \equiv 2\ (mod\ 503)$$

$$9\,x \equiv 21\ (mod\ 30) \quad ، \quad 79\,x \equiv 2\ (mod\ 153)$$

$$17\,x \equiv 9\ (mod\ 276) \quad ، \quad 182\,x \equiv 7\ (mod\ 203)$$

$$4\,x \equiv 9\ (mod\ 51) \quad ، \quad 140\,x \equiv 133\ (mod\ 301)$$

١٧- أوجد أصغر عدد صحيح موجب باقي قسمته على 13 يساوي 5 وباقي قسمته على 12 يساوي 3 وباقي قسمته على 35 يساوي 2 .

١٨- أوجد الحل المشترك لكل من جمل التطابقات التالية :

a) $x \equiv 3\ (mod\ 6)$ ، $x \equiv -1\ (mod\ 25)$ ، $x \equiv 1\ (mod\ 7)$

b) $x \equiv -2\ (mod\ 11)$ ، $x \equiv 13\ (mod\ 28)$ ، $x \equiv 7\ (mod\ 45)$

c) $5x \equiv 2\ (mod\ 13)$ ، $x \equiv 2\ (mod\ 35)$

$3x \equiv 13\ (mod\ 77)$ ، $x \equiv 7\ (mod\ 20)$

d) $17x \equiv 3\ (mod\ 7)$ ، $17x \equiv 3\ (mod\ 5)$

$17\,x \equiv 3\ (mod\ 2)$ ، $17x \equiv 3\ (mod\ 3)$

١٩- أوجد أصغر عدد صحيح $a>2$ بحيث تتحقق العلاقات :

$$2 \mid a \quad , \quad 3 \mid a+1 \quad , \quad 4 \mid a+2 \quad , \quad 5 \mid a+3 \quad , \quad 6 \mid a+4$$

٢٠- أوجد باقي قسمة $2(26!)$ على 29 .

٢١- رتب الأعداد $2, 3, 4, \ldots, 21$ وفق ثنائيات (a, b) بحيث $a.b \equiv 1 (mod\, 23)$.

٢٢- أثبت أن $18! \equiv -1 (mod 23)$.

٢٣- إذا كان p عدداً أولياً أثبت أن :

$$p \mid a^p + (p-1)!\, a \quad \text{و} \quad p \mid (p-1)!\, a^p + a$$

٢٤- أوجد العدد الصحيح x بحيث يكون :

$$3^2 \mid x \quad , \quad 4^2 \mid x+1 \quad , \quad 5^2 \mid x+2$$

الفصل الثالث

الدوال العددية أو الحسابية وبعض الدوال الخاصة

- تعريف الدوال العددية
- الدالة الضربية
- دالة الجزء الصحيح وخواصها
- مجموعة البواقي المختزلة
- دالة أولر φ ودالة أولر المعممة ψ
- الدالتان σ, τ
- الأعداد التامة
- دالة موبياس وصيغة موبياس للتعاكس
- دالة ليوفيل λ ودالة مانجولد $\wedge$

٢-٣ الدوال العددية وبعض الدوال الخاصة في نظرية الأعداد

٢-٣-١ تعريف : الدوال العددية (*Number - Theoretic Functions*)

- أو الدوال الحسابية « ***arithmetic functions*** » هي الدوال التي مجال تعريفها الأعداد الصحيحة الموجبة ، ولهذه الدوال أهمية عظمى في نظرية الأعداد وسندرس في هذا الفصل عدداً من هذه الدوال التي قيمها أعداد صحيحة وندرس خواصها .

٢-٣-٢ الدالة العددية الضربية :

نقول إن الدالة العددية f دالة ضربية إذا حققت الشرطين :

١- f غير صفرية

٢- $\forall\, a , b \in Z^{+}$ و $(a , b)=1$ فإن :

$$f(a.b)=f(a).f(b)$$

ونقول إن الدالة f ضربية تماماً إذا حققت الشروط السابقة دون الشرط $(a , b)=1$.

مثال : الدالة المعرفة بـ : $f_{\alpha}(n)=n^{\alpha}$ (حيث $\alpha , n \in Z^{+}$) . ضربية تماماً ، لأن :

١- $f_{\alpha}(n)\neq 0$ مهما تكن $n>0$

٢- إذا كان $n_1 , n_2 \in Z^{+}$ فإن :

$$f_{\alpha}(n_1.n_2)=(n_1.n_2)^{\alpha}=n_1^{\alpha}.n_2^{\alpha}=f_{\alpha}(n_1).f_{\alpha}(n_2)$$

٢-٣-٣ مبرهنة : إذا كانت f دالة ضربية فإن $f(1)=1$

البرهان : بما أن الدالة f ضربية فإنها غير صفرية أي يوجد عدد n بحيث يكون $f(n)\neq 0$

ولما كان $(n, 1)=1$ و $f(n.1)=f(n).f(1)$ فإن $f(1)=1$

- نتيجة (١) : يمكن أن نعرف الدالة العددية الضربية بأنها الدالة العددية التي تحقق الشرطين :

١- $f(1)=1$

٢- $f(a.b)=f(a).f(b)$ حيث $(a,b)=1$, $a,b\in Z^+$.

- نتيجة (٢) : إذا كانت الدالة f دالة عددية ضربية وكانت الأعداد $n_1,n_2,...,n_r$ أولية نسبياً مثنى مثنى ، فإن :

$$f(n_1.n_2.....n_r)=f(n_1).f(n_2).....f(n_r)$$

البرهان : نبرهن صحة هذه النتيجة بطريقة الاستقراء :

١- من أجل $r=2$ نجد أن $(n_1,n_2)=1$ و $f(n_1.n_2)=f(n_1).f(n_2)$

٢- لنفترض أن العبارة صحيحة عندما $r=k$ ولنثبت صحتها من أجل $r=k+1$

بما أن $((n_1.n_2.....n_k),n_{k+1})=1$ وبما أن :

$$f(n_1.n_2.....n_k)=f(n_1).f(n_2).....f(n_k)$$

نجد :

$$f((n_1.n_2...n_k).n_{k+1})=f(n_1.n_2...n_k).f(n_{k+1})$$
$$=f(n_1).f(n_2)...f(n_k).f(n_{k+1})$$

أي العبارة صحيحة من أجل $r>1$

- نتيجة : إذا كانت f دالة ضربية و كانت العبارة القانونية للعدد n هي : $n=p_1^{\alpha_1}p_2^{\alpha_2}.....p_k^{\alpha_k}$ فإن $f(n)=f(p_1^{\alpha_1}).f(p_2^{\alpha_2}).....f(p_k^{\alpha_k})$

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 : $\sum_{d|15} f(d)=f(1)+f(3)+f(5)+f(15)$

٢-٣-٤ تمهيدية (١) : إذا كانت f , g دالتين عدديتين فإن :

$$\sum_{\substack{d\mid m\\ e\mid n}} f(d)\,g(e)=\left(\sum_{d\mid m} f(d)\right)\left(\sum_{e\mid n} g(e)\right)$$

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 :

$$\sum_{\substack{d\mid m\\ e\mid n}} f(d)\,g(e)=\sum_{\substack{j=1,\ldots,s\\ k=1,\ldots,t}} f(d_j)\;g(e_k)$$

$$=\sum_{j=1}^{s} f(d_j)g(e_1)+\sum_{j=1}^{s} f(d_j)g(e_2)+\ldots+\sum_{j=1}^{s} f(d_j)g(e_t)$$

$$=\left(\sum_{j=1}^{s} f(d_j)\right)\left(\sum_{k=1}^{t} g(e_k)\right)=\sum_{d\mid m} f(d)\,.\sum_{e\mid n} g(e)$$

وهو المطلوب .

٢-٣-٥ تمهيدية (٢) : 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

$$m=p_1^{\alpha_1}p_2^{\alpha_2}\ldots\ldots p_s^{\alpha_s} \quad \text{و} \quad n=q_1^{\beta_1}q_2^{\beta_2}\ldots\ldots q_r^{\beta_r}$$

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 :

$$d=p_1^{c_1}p_2^{c_2}\ldots\ldots p_s^{c_s}\quad q_1^{t_1}q_2^{t_2}\ldots\ldots q_r^{t_r}$$

حيث $0\le c_i\le \alpha_i$ $\quad$ $0\le t_i\le \beta_i$

أي يمكن أن نكتب : $d=d_1.d_2$

حيث $d_1 = p_1^{c_1} p_2^{c_2} \dots p_s^{c_s} \quad , \quad d_2 = q_1^{t_1} q_2^{t_2} \dots q_r^{t_r}$

إن $d_1 | m \quad , \quad d_2 | n$ ولايوجد أي عامل مشترك بين d_2 و d_1

أي أنّ : $(d_1, d_2) = 1$.

٢-٣-٦ 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 : $F(1) = 1$ محقق وضوحاً.

لنفترض n , m عددين صحيحين موجبين وأن $(m,n) = 1$ ولنكتب :

$$F(m.n) = \sum_{d|mn} f(d) = \sum_{\substack{d_1|m \\ d_2|n}} f(d_1 d_2)$$

لأن أي قاسم d للجداء $m.n$ يكتب بشكل وحيد كجداء قاسم لـ $d_1 : m$ وقاسم لـ $d_2 : n$ 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 :

$$F(m.n) = \sum_{\substack{d_1|m \\ d_2|n}} f(d_1).f(d_2) = \left(\sum_{d_1|m} f(d_1)\right)\left(\sum_{d_2|n} f(d_2)\right)$$

$$\Rightarrow \quad F(m.n) = F(m)\ F(n)$$

مثال : لنوضح المبرهنة السابقة بالمثال التالي : حيث نأخذ $n = 3$ ، $m = 8$ و $mn = 24$ ، فتكون قواسم n هي $\{1, 3\}$ وقواسم m هي $\{1, 2, 4, 8\}$

$$F(8 \times 3) = \sum_{d|24} f(d)$$

$$= f(1) + f(2) + f(3) + f(4) + f(6) + f(8) + f(12) + f(24)$$

$$=[\ f(1)+f(2)+f(4)+f(8)\ ][\ f(1)+f(3)]$$

تمرين : لتكن الدالة g المعرفة على النحو التالي :

$$g(n)=\begin{cases}0 & n \text{ زوجي}\\ 1 & n \text{ فردي}\end{cases}$$

ولتكن $G(n)=\sum_{d|n} g(d)$

١- برهن أن g و G دالتان ضربيتان : إن : $g(1)=1$ و إذا كان $(m,n)=1$ فإن

$$g(n.m)=\begin{cases}0 & \text{أحدهما زوجي}\\ 1 & \text{كلاهما فردي}\end{cases} \quad \text{أي} \quad g(n.m)=g(n)\ g(m)$$

و g دالة ضربية وكذلك G حسب المبرهنة السابقة .

٢- أوجد قيمة $G(p^k)$ حيث p عدد أولي فردي :

لدينا

$$g(1)+g(p)+g(p^2)+.....+g(p^k)=k+1$$
$$G(p^k)=\sum_{d|p^k} g(d)=k+1$$

لأن قوى أي عدد فردي هي أعداد فردية .

٣- احسب $G(20)$: $G(220)$

- $G(20)=\sum_{d|20} g(d)=g(1)+g(2)+g(4)+g(5)+g(10)+g(20)$
$=2$

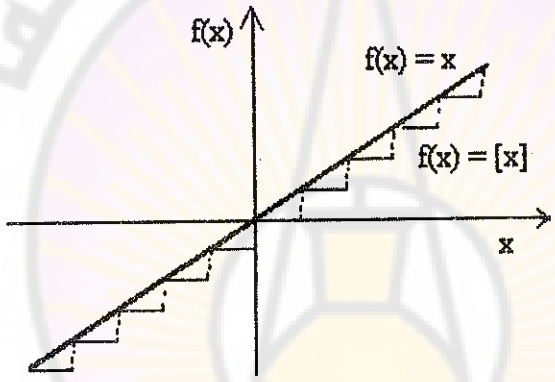
- إن القواسم الفردية لـــ 220 هي 5 , 11 , 55 وبالتالي فإن $G(220)=3$.

٢-٣-٧ 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 وترمّز $[\alpha]$ بأنها أكبر عدد صحيح لا تتجاوز قيمته قيمة العدد α (يُرمَّز أحيانـــاً $\lfloor\alpha\rfloor$ ليتميز عن العدد الصحيح الذي هو أكبر مباشرة من α والذي يُرمَّـــز $\lceil\alpha\rceil$) .

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 :

$$\alpha = [\alpha]+\theta \qquad 0 \le \theta < 1$$

ويسمى العدد θ الجزء الكسري من α .

أمثلة :

$$\left[-\sqrt{10}\right]=-4 \ , \ [2.5]=2 \ , \ \left[-\frac{12}{5}\right]=-3 \ , \ \left[\sqrt{10}\right]=3 \ , \ [-0.5]=-1$$

٢-٣-٨ خواص دالة الجزء الصحيح

١) إذا كان $\alpha \in \Re$, $k \in Z$ فإن :

$$[\,k+\alpha\,]=k+[\alpha\,]$$

البرهان : لدينا : $[\,k+\alpha\,] \le k+\alpha < [\,k+\alpha\,]+1$

$$(\,[\,k+\alpha\,]-k\,) \le \alpha < (\,[\,k+\alpha\,]-k)+1$$

أي أن $[\,\alpha\,]=[\,k+\alpha\,]-k$ وبالتالي : $[\,k+\alpha\,]=[\,\alpha\,]+k$

٢) إذا كان $\alpha \in \Re$, $n \in Z^{+}$ فإن :

$$\left[\frac{[\alpha]}{n}\right]=\left[\frac{\alpha}{n}\right]$$

البرهان :

لدينا : $0 \le \theta < 1$: $\frac{\alpha}{n}=\left[\frac{\alpha}{n}\right]+\theta$

ومنه $\alpha = n\left[\frac{\alpha}{n}\right]+n\theta$

$$[\alpha]=n\left[\frac{\alpha}{n}\right]+[n\theta] \quad : \ 0 \le n\theta < n$$

أي $\frac{[\alpha]}{n}=\left[\frac{\alpha}{n}\right]+\frac{[n\theta]}{n}$: $0\le[n\theta]<n\theta<n$

ومنه $\left[\frac{[\alpha]}{n}\right]=\left[\frac{\alpha}{n}\right]+0$: $0\le\frac{[n\theta]}{n}<1$

- نتيجة :

إن $\left[\frac{\left[\alpha/n\right]}{m}\right]=\left[\frac{\alpha}{n\,.\,m}\right]$ حيث $\alpha\,,\,n\,,\,m\in Z^{+}$

٣) إذا كان n عدداً صحيحاً أكبر من الواحد و α عدداً حقيقياً أكبر أو يساوي الواحد فإن :

$$[\alpha]>\left[\frac{\alpha}{n}\right]$$

البرهان : نكتب : $\frac{\alpha}{n}=\left[\frac{\alpha}{n}\right]+\theta$: $0\le\theta<1$

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 $n>1$, $0\le[n\theta]$

٤) إذا كان $a\,,\,b,\,n\in Z^{+}$ فإن $\left[\frac{a\,b}{n}\right]\ge a\left[\frac{b}{n}\right]$

البرهان : لدينا من تعريف دالة الجزء الصحيح :

$$\frac{b}{n}=\left[\frac{b}{n}\right]+\theta \qquad : \qquad 0\le\theta<1$$

$$\frac{a\,b}{n}=a\left[\frac{b}{n}\right]+a\theta \qquad : \quad 0\le a\theta<a$$

$$\left[\frac{a\,b}{n}\right]=a\left[\frac{b}{n}\right]+[a\theta]\ge a\left[\frac{b}{n}\right]$$

٥) إذا كانت الأعداد $\alpha_i\in\Re$ و $\alpha=\sum_1^k\alpha_i$ فإن :

$$[\alpha]\ge\sum_1^k[\alpha_i]$$

البرهان : نكتب

$$\alpha_1=[\alpha_1]+\theta_1 \qquad 0\le\theta_1<1$$

$$\alpha_i=[\alpha_i]+\theta_i \qquad 0\le\theta_i<1$$

$$\alpha_n=[\alpha_n]+\theta_n \qquad 0\le\theta_n<1$$

بالجمع نجد

$$\alpha=\sum_1^n[\alpha_i]+\sum_1^n\theta_i \Rightarrow [\alpha]=\sum_1^n[\alpha_i]+\left[\sum_1^n\theta_i\right]$$

ولما كانت θ_i كلها أعداد موجبة فإن $[\alpha]\ge\sum_1^n[\alpha_i]$

- **نتيجة (١):** $[x,y]\ge[x]+[y] \quad \forall x,y\in\Re$
- **نتيجة (٢) :** ينتج من الخاصة الأخيرة مباشرة أن :

$$\left[\frac{n}{p}\right]\ge\left[\frac{n_1}{p}\right]+\left[\frac{n_2}{p}\right]+\ldots\ldots+\left[\frac{n_k}{p}\right]$$

حيث p عدد صحيح غير الصفر و n_i أعداد صحيحة و $n=\sum_{1}^{k} n_i$.

٢-٣-٩ مبرهنة : إذا كان $n \in Z^+$ و p عدداً أولياً فإن أس أكبر قوة لـ p تقسم $n!$ (ويرمّز $H_p(n!)$) يساوي :

$$H_p(n!) = \left[\frac{n}{p}\right]+\left[\frac{n}{p^2}\right]+.....+\left[\frac{n}{p^k}\right] = \sum_{i=1}^{\infty}\left[\frac{n}{p^i}\right]$$

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 وهي مضاريب "$n!=1.2....n$" كما يلي :

$$1,2,....,p,p+1,....,2p,....,3p,.....,pp,p^2+1,....,2p^2,....pp^2,...,n$$

لنفترض أن الأعداد التي تقبل القسمة على p من بين هذه الأعداد هي :

$p,2p,...,t_1p$ حيث t_1 هو أكبر عدد صحيح يحقق العلاقة $t_1p\leq n$. 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:

$p,2p,3p,...,\left[\frac{n}{p}\right]p$ ، وبمحاكمة شبيهة نجد أن عدد الأعداد التي تقبل القسمة على p^2 من بين مضاريب $n!$ هو $t_2=\left[\frac{n}{p^2}\right]$ وهي:

$$p^2,2p^2,...,\left[\frac{n}{p^2}\right]p^2$$

ومن بين هذه الأعداد يوجد $\left[\frac{n}{p^3}\right]$ عدداً يقبل القسمة ثانية على p أي يقبل القسمة على p^3 ، وهكذا بعد تكرار هذه المحاكمة عدداً منتهياً من المـــرات نجد أن عدد المرات التي يقسم بها p العدد $n!$ هو :

$$\left[\frac{n}{p}\right]+\left[\frac{n}{p^2}\right]+.....+\left[\frac{n}{p^k}\right]=t_1+t_2+...+t_k$$

أي أن $n!$ تقبل القسمة على $p^{t_1+t_2+...+t_k}$ ومنه $H_p(n!)=\sum_{i=1}^{\infty}\left[\frac{n}{p^i}\right]$

مثال (١) : لنوضح المبرهنة السابقة بالمثال التالي : إذا كان $p=3$ و $n=19$

فإن $19!=1.2.3....6..9....12...15.....18.19$

مضاعفات العدد 3 من بين مضاريب $19!$ هي $\{3,6,9,12,15,18\}$

وعددها $\left[\frac{19}{3}\right]=6$.

مضاعفات العدد 3^2 هي $\{9,18\}$ عددها $\left[\frac{19}{9}\right]=2$ وعدد مضاعفات العدد $3^3=27$ صفر أي $H_3(19!)=6+2=8$ و $3^8|19!$ فـــي حـــين $3^9 \nmid 19!$.

تمرين : ما هو عدد الأصفار في نهاية العدد $50!$

الحل: لتعيين عدد الأصفار في نهاية $50!$ لنبحث عن أكبر قوة للعـــدد 10 تقسم $50!$ ولكن $10=2.5$ لذا نبحث عن $H_2(50!)$ و $H_5(50!)$

فنجد :

$$H_2(50!)=\left[\frac{50}{2}\right]+\left[\frac{50}{4}\right]+\left[\frac{50}{8}\right]+\left[\frac{50}{16}\right]+\left[\frac{50}{32}\right]+\left[\frac{50}{64}\right]$$

$$=25+12+6+3+1+0=47$$

ومنه نجد : $2^{47}|50!$ و $2^{48} \nmid 50!$

$$H_5(50!) = \left[\frac{50}{5}\right] + \left[\frac{50}{25}\right] + 0 = 10 + 2 = 12 \Rightarrow 5^{13} \nmid 50! \quad \text{و} \quad 5^{12} \mid 50!$$

ولما كان $(2,5)=1$ فإن أس أكبر قوة للعدد 10 تقسم !50 هو 12 وعدد الأصفار في نهاية !50 هو 12 .

٢-٣-١٠ 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 :

$$H_p(m!) = \left[\frac{m}{p}\right] + \left[\frac{m}{p^2}\right] + \ldots + \left[\frac{m}{p^r}\right]$$

$$= a_r p^{r-1} + a_{r-1} p^{r-2} + \ldots\ldots\ldots\ldots + a_1 +$$

$$+ a_r p^{r-2} + a_{r-1} p^{r-3} + \ldots + a_2 +$$

$$+ \ldots\ldots\ldots\ldots$$

$$\ldots\ldots\ldots\ldots$$

$$+ a_r p + a_{r-1}$$

$$+ a_r$$

ومنه

$$H_p(m!) = a_r(1 + p + p^2 + \ldots + p^{r-1}) + a_{r-1}(1 + p + p^2 + \ldots + p^{r-2}) + \ldots + a_1$$

$$H_p(m!) = a_r \frac{p^r - 1}{p-1} + a_{r-1} \frac{p^{r-1} - 1}{p-1} + \dots + a_2 \frac{p^2 - 1}{p-1} + a_1$$

$$H_p(m!) = \frac{a_r p^r + a_{r-1} p^{r-1} + \dots + a_1 p + a_0 - (a_r + a_{r-1} + \dots + a_2 + a_1 + a_0)}{p-1}$$

$$H_p(m!) = \frac{m - \sum_0^r a_i}{p-1}$$

مثال : اكتب العدد 347 بنظام العد الذي أساسه 7 ثم احسب $H_7(347!)$

الحل : $347 = 1(7^3) + 0(7^2) + 0(7) + 4 = (1004)_7$

وبتطبيق المبرهنة الأخيرة نجد : $H_7(347!) = \frac{347-(5)}{7-1} = 57$

٢-٣-١١ مبرهنة : إذا كان n و r عددين صحيحين وكان $1 \le r < n$

فإن : $\binom{n}{r} = \frac{n!}{r!(n-r)!}$ هو عدد صحيح

البرهان : من أجل البرهان يكفي أن نثبت أن أس أكبر قوة لأي عدد أولي p يقسم المقام أصغر أو يساوي أس أكبر قوة لهذا العدد الأولي p تقسم البسط لذا نكتب حسب الخاصة (٥) من خواص دالة الجزء الصحيح :

$$\left[\frac{n}{p^k}\right] \ge \left[\frac{r}{p^k}\right] + \left[\frac{n-r}{p^k}\right]$$

وبالجمع على k نجد :

$$\sum_{k\ge1} \left[\frac{n}{p^k}\right] > \sum_{k\ge1} \left[\frac{r}{p^k}\right] + \sum_{k\ge1} \left[\frac{n-r}{p^k}\right]$$

ومنه

$$H_p(n!) \ge H_p(r!\,(n-r)!)$$ (برر ذلك)

أي أن أي عامل للمقام يقسم البسط والناتج عدد صحيح .

- **نتيجة :** إن جداء n من الأعداد الصحيحة المتتالية الموجبة يقبل القسمة على $n!$

البرهان :

لنكتب :

$$\frac{(k+1)(k+2).....(k+n)}{n!} = \frac{k!\,(k+1).....(k+n)}{k!\,.\,n!}$$

$$= \frac{(k+n)!}{k!\;\;n!} = \text{عدد صحيح}$$

- **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 $2m = m + m$ و $3n = n + n + n$ بالتالي ينتج أن :

$\frac{(2m)!}{m!\,m!}$ و $\frac{(3n)!}{(n!)(n!)(n!)}$ عددان صحيحان و جداؤهما عدد صحيح.

٢-٣-١٢ 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 : 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 $N \geq$ 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 $1, 2, \ldots\ldots, N$ التي تقبل القسمة على k . إن هذا العدد كما سبق ورأينا يساوي $\left[\frac{N}{k}\right]$. وهذه الأعداد هي $k, 2k, 3k, \ldots, \left[\frac{N}{k}\right]k$ وهكذا نجد أنه من أجل كل عدد k حيث $1 \leq k \leq N$ يكون $f(k)$ هو حد في المجموع $\sum_{d|n} f(d)$ وذلك من أجل $\left[\frac{N}{k}\right]$ من الأعداد الصحيحة الموجبة المختلفة التي هي أصغر أو تساوي 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 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 عدديتين وكان $F(n) = \sum_{d|n} f(d)$ و $\alpha \in \Re$.

$$\sum_{n=1}^{\alpha} F(n) = \sum_{n=1}^{[\alpha]} \sum_{d|n} f(n) \quad .$$

٢-٣-١٣ 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 $A=\{0, 1, 2, \ldots, m-1\}$

مثال (١) : 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 (٢) : 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 بالمقاس 12 .

ومن الواضح أن عدد عناصر أي مجموعتي بواقي مختزلة بالمقاس m متساوٍ.

٢-٣-١٤ دالة أولر φ. *Euler's φ - 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 بواقي مختزلة بالمقاس m .

مثال : $\varphi(1)=1$, $\varphi(2)=1$, $\varphi(3)=2$ لأن الأعداد التي هي ≥ 3 والأولية نسبياً مع 3 هي 1 , 2 ، حيث : $T(3)=\{1, 2\}$ وعدد عناصر $T(3)$ هو 2 $\varphi(3)=$ ، لإيجاد $\varphi(5)$ نكتب :

$$T(5)=\{1,2,3,4\} \quad \text{و} \quad A(5)=\{0,1,2,3,4\}$$

وعدد عناصر $T(5)$ هو 4 أي : $\varphi(5)=4$.

٢-٣-١٥ مبرهنة : إن دالة اولر دالة عددية ضربية .

البرهان : ١- إن $\varphi(1)=1$ حسب تعريف الدالة .

٢ - 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 مساوياً للواحد فالمبرهنة صحيحة لـذا لنفترض أن $a>1$ و $b>1$ و لنرتب الأعداد من 1 إلى $a\,b$ كما يلي :

$0.a+1$	2	3	....	r	....	a
$1.a+1$	$a+2$	$a+3$	....	$a+r$	....	$2a$
$2.a+1$	$2a+2$	$2a+3$	....	$2a+r$	....	$3a$
....	....	....	....	....	....	....
$q\ a+1$	$q\ a+2$	....	....	$q\,a+r$	....	$(q+1)a$
....	....	....	....	....	....	....
$(b-1)\ a+1$	$(b-1)\ a+2$	....	....	$(b-1)\ a+r$	....	$b\,a$

نلاحظ أن عناصر كل سطر في هذه المصفوفة تشكل مجموعة بواق تامـة بالمقاس a وأن عناصر كل عمود تشكل مجموعة بواق تامـة بالمقـاس b إذ نلاحظ أن عدد عناصر كل سطر يساوي a وأن أي عنصرين مختلفين غيـر متطـابقين بالمقـاس a لأنـه لـو كـان : $q\,a+s\equiv q\ a+t(mod\ a)$ لنـتج $s\equiv t(mod\ a)$ وهذا غير ممكن إن كان العنصران مختلفين،وبشكل مشابه نجد أن عدد عناصر كل عمود يساوي b وأنه لو كان : $q\,a+r\equiv q_1a+r(mod\,b)$ لنتج $q\,a\equiv q_1a\ (mod\,b)$ ولما كان $(a,b)=1$ فإن هذا يؤدي إلى : $q\equiv q_1(mod\,b)$ وهذا غير ممكن من أجل أي عنصرين مختلفين من العمود .

ومن جهة أخرى نعلم أن عدد العناصر الأولية نسبياً مع a في كل سطر يساوي $\varphi(a)$ وأن العنصر $((qa+r), a)=1$ إذا وفقط إذا كان $(r, a)=1$ لذا نأخذ أي عمود r يحقق الشرط $(r, a)=1$ ونلاحظ أن عدد عناصر هذا العمود الأولية نسبياً مع b يساوي $\varphi(b)$ مما يدل على أن عدد العناصر من المصفوفة السابقة التي هي أولية نسبياً 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 :

$$\varphi(12)=\varphi(3).\varphi(4)=(2)(2)=4$$

$$\varphi(15)=\varphi(3).\varphi(5)=(2)(4)=8$$

٢-٣-١٦ 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 : $\varphi(p)=p-1$

٢-٣-١٧ مبرهنة : إذا كان p عدداً أولياً فإن :

$\varphi(p^{\alpha})=p^{\alpha-1}(p-1)=p^{\alpha}-p^{\alpha-1}$ حيث $\alpha>0$

البرهان : إن مجموعة البواقي التامة للعدد p^{α} هي :

$$A=\{1,2,....,p,p+1,....,2p,....,p^2.....,p^{\alpha-1},2p^{\alpha-1},...,p.p^{\alpha-1}\}$$

وعناصر A التي لها عامل مشترك مع p^{α} هي $p,2p,....,p^{\alpha-1}p$ 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 : $\varphi(8) = \varphi(2^3) = 2^3(2-1) = 4$

٢-٣-١٨ مبرهنة : إذا كان n عدداً صحيحاً موجباً $n>1$ وكان :

$$n = p_1^{\alpha_1} \; p_2^{\alpha_2} \ldots p_r^{\alpha_r}$$

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 :

$$\varphi(n) = \varphi(p_1^{\alpha_1})\,\varphi(p_2^{\alpha_2}) \ldots\ldots \varphi(p_r^{\alpha_r})$$

$$= p_1^{\alpha_1} \; p_2^{\alpha_2} \ldots p_r^{\alpha_r} \; (1-\frac{1}{p_1}) \ldots\ldots (1-\frac{1}{p_r})$$

$$\varphi(n) = n(1-\frac{1}{p_1}) \ldots\ldots (1-\frac{1}{p_r})$$

مثال :

$$\varphi(360) = \varphi(2^3 . 3^2 . 5) = 360 \;\; (1-\frac{1}{2})(1-\frac{1}{3})\;(1-\frac{1}{5})$$

$$\varphi(360) = 96$$

٢-٣-١٩ مبرهنة أولر : إذا كان $(a, m) = 1$ فإن :

$$a^{\varphi(m)} \equiv 1 \,(mod\, m)$$

البرهان : إذا كانت $T = \{ a_1, a_2, \ldots\ldots, a_{\varphi(m)} \}$ مجموعة بواق مختزلة بالمقاس m ، فإن المجموعة

$$T_1 = \{ a_1 a, a_2 a, \ldots\ldots, a_{\varphi(m)} . a \}$$

هي أيضاً مجموعة بواق مختزلة بالمقاس m ، إذ أن كل عنصر من T_1 أولي نسبياً مع m وضوحاً كما أن أي عنصرين من T_1 غير متطابقين بالمقاس m ، لأنه لو كان $a_i . a \equiv a_j . a \pmod m$ لكان $a_i \equiv a_j \pmod m$ وهـذا مـستحيل لأنها عناصر من T . وبالتالي فإن كل عنصر من T يطابقه عنصر واحـد فقط من T_1 الأمر الذي يؤدي إلى أن جداء عناصر T يطابق جداء عناصـر T_1 بالمقاس m ونكتب

$$a_1 . a_2 ..... a_{\varphi(m)} \equiv a_1 . a_2 ..... a_{\varphi(m)} . a^{\varphi(m)} \pmod m$$

ولما كان $(a_1 . a_2 ..... a_{\varphi(m)}, m) = 1$ فإن :

$$a^{\varphi(m)} \equiv 1 \pmod m$$

مثال : $a^{\varphi(15)} \equiv 2^8 \equiv 1 \pmod{15}$

٢-٣-٢٠ نتيجة : إن مبرهنة فيرما الصغرى هي حالة خاصة من مبرهنة أولر إذ لو كان المقاس p عدداً أولياً لحصلنا على :

$$a^{\varphi(p)} \equiv a^{p-1} \equiv 1 \pmod p$$

تمرين : أوجد رقمي الآحاد والعشرات للعدد 3^{256} .

الحل: إن العدد المؤلف من رقمي الآحاد والعشرات يساوي باقي قسمة 3^{256} على العدد 100 ولما كان $(3, 100) = 1$ فـإن $3^{\varphi(100)} \equiv 1 \pmod{100}$

نحسب $\varphi(100)$ فنجد :

$$\varphi(100) = \varphi(2^2 . 5^2) = 100 (1 - \frac{1}{2}) (1 - \frac{1}{3}) = 40$$

أي : $3^{40} \equiv 1 \pmod{100}$

ولدينا $256 = (40)(6) + 16$ لذا نكتب :

$$3^{256} \equiv (3^{40})^6 . 3^{16} \equiv 3^{16} \pmod{100} \equiv (81)^4 \equiv (-19)^4 \pmod{100}$$

$$3^{256} \equiv (361)^2 \equiv (61)^2 \equiv 21 \pmod{100}$$

والرقمان المطلوبان يعطيان 21 .

٢-٣-٢١ تطبيق هام : يمكن استخدام مبرهنة اولر في إيجاد حلول التطابقات الخطية

مثال : لنوجد حلول التطابق $6x \equiv 15 \pmod{21}$

نلاحظ أن $(6,21)=3$, $3|15$ أي أن للتطابق ثلاثة حلول غير متطابقة بالمقاس 21 . نختصر طرفي التطابق على 3 فنجد :

$$2x \equiv 5 \pmod{7}$$

ولدينا $\varphi(7)=6$ ، نضرب طرفي التطابق بـ 2^5 فنجد :

$$2^6 . x \equiv 5 . 2^5 \pmod{7}$$

وحسب مبرهنة أولر $2^6 \equiv 1 \pmod{7}$ مما يعطي

$$x \equiv 5 . 2^5 \pmod{7} \equiv 5 . 2^3 . 2^2 \pmod{7} \equiv 5 . 2^2 \pmod{7}$$

$$x \equiv 20 \pmod{7} \equiv 6 \pmod{7}$$

وجميع حلول التطابق غير المتطابقة بالمقاس 21 هي :

$$x = 6 + 7t \quad ; \quad t = 0,1,2$$

أي هي : 6 , 13 , 20

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 $d|n$ نجد $n = d\ d_1$, $d_1 = \frac{n}{d} | n$.

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 .

٢-٣-٢٢ مبرهنة : إذا كان $n \geq 1$ فإن $n = \sum_{d \mid n} \varphi(d)$.

البرهان : لنوزع الأعداد من 1 إلى n في 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 $\varphi \left(\frac{n}{d} \right)$.

ولما كان كل من الأعداد $\{ 1 , 2 , ..., n \}$ ينتمي إلى صف واحد فقط من الصفوف S_d . فإننا نجد أن $n = \sum_{d \mid n} \varphi \left(\frac{n}{d} \right) = \sum_{d \mid n} \varphi \ (d)$

مثال (١) : 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" $= \varphi \left(\frac{10}{2} \right) = \varphi \ (5) = 4$

$$S_5 = \{\ m\ :\ (m,10)=5\ \ ,\ \ \ 1 \le m \le 10\ \} = \{5\}$$

"عدد عناصر S_5" $= 1 = \varphi\ (\frac{10}{5})$

$$S_{10} = \{\ m\ :\ (m,10)=10\ \ ,\ \ \ 1 \le m \le 10\ \} = \{10\}$$

"عدد عناصر S_{10}" $= 1 = \varphi\ (1) = \varphi\ (\frac{10}{10})$

وبالتالي :

$$n = \varphi\ (10) + \varphi\ (5) + \varphi\ (2) + \varphi\ (1) = 4+4+1+1 = 10$$

مثال (٢) : إذا كان $n = 25$ فإن قواسم العدد 25 هي $\{25, 5, 1\}$

$$S_1 = \{m : (m,25) = 1\ ,\ 1 \le m \le 25\ \} \rightarrow \varphi(25) = \varphi(5^2)$$

"عدد عناصر S_1" $= 5(5-1) = 20 =$

$$S_5 = \{m : (m,25) = 5\ ,\ 1 \le m \le 25\ \} \Rightarrow \varphi(\frac{25}{5}) = \varphi(5) = 4$$

"عدد عناصر S_5" $= 4$

$$S_{25} = \{25\} \qquad \Rightarrow \quad \varphi(\frac{25}{25}) = \varphi(1) = 1 =$$ "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 :

$$\varphi(22) = \varphi(11).\varphi(2) = 10 \quad \text{و} \quad 3^{\varphi(22)} \equiv 5^{\varphi(22)} \equiv 1\ (mod\ 22)$$

ومنه : $(5^{10})^n \equiv 1\ (mod\ 22)$ و $(3^{10})^n \equiv 1\ (mod\ 22)$

نعوض في عبارة $f(n)$ فنجد :

$$f(n) \equiv 3^{10n+2} + 5^{10n+3} - 2 \equiv 3^2 + 5^2 - 2 \equiv 132 \equiv 0\ (mod\ 22)$$

٢-٣-٢٣ دالة أولر المعممة المرتبطة بأعداد صحيحة مفروضة ψ :

- تعريف : لقد عرف العالم لوقا ($E.Lucas$) هذه الدالة كما يلي :

لتكن $e_1, e_2, \ldots, e_k$ أعداداً صحيحة . وليكن $n \geq 1$ إن الرمز $\psi(n, e_1, e_2, \ldots, e_k)$ أو $\psi(n)$ يمثل عدد الأعداد الصحيحة h من بين الأعداد $1, 2, \ldots, n$ التي تحقق الخاصة التالية $(h + e_i, n) = 1$ من أجل $i = 1, 2, \ldots, k$.

ويلاحظ أنه إذا كانت $e_i = 0$ حيث $i = 1, 2, \ldots, k$ فإن $\psi(n) = \varphi(n)$.

مثال : لنأخذ $n = 15$ و $e_2 = 1$, $e_1 = 0$ إن $\psi(15, 0, 1)$ يرمز إلى عدد الأعداد h حيث $1 \leq h \leq 15$ التي تحقق:

$$(h, 15) = 1 \quad \text{و} \quad (h+1, 15) = 1$$

إن الأعداد التي تحقق $(h, 15) = 1$ هي :

$1, 2, 4, 7, 8, 11, 13, 14$ ومن بين هذه الأعداد نختار الأعداد التي تحقق $(h+1, 15) = 1$ وهي : 13 , 7 , 1 وعددها 3 إذن :

$$\psi(15, 0, 1) = 3$$

٢-٣-٢٤ مبرهنة (للإطلاع) : إن دالة أولر المعممة ضربية.

الإثبات : ١) لدينا $\psi(1) = 1$

٢) لنثبت أن $\psi(m.n) = \psi(m).\psi(n)$ عندما $(m, n) = 1$

لنأخذ العددين s, r بحيث يكون :

$$r \equiv 1 \ (mod\ m) \qquad r \equiv 0 \ (mod\ n)$$

$$s \equiv 0 \ (mod\ m) \qquad s \equiv 1 \ (mod\ n)$$

فإذا مسح العدد الصحيح x جميع عناصر مجموعة البواقي التامة بالمقاس m أي القيم $1, 2, \ldots, m$ ومسح العدد الصحيح y جميع عناصر مجموعة بواق تامة بالمقاس n أي القيم $1, 2, \ldots, n$ بشكل مستقل عن x فإن العدد الصحيح

z المعرف بالعلاقة $z = r\,x + s\,y (mod\ mn)$ يمسح جميع عناصر مجموعة البواقي التامة بالمقاس $m \cdot n$.

لأنه إذا كان $r\,x' + s\,y' \equiv r\,x'' + s\,y''\ (mod\ mn)$

فإن : $r\,(x' - x'') \equiv s(y'' + y')\ (mod\ mn)$ أي :

$$r(x' - x'') \equiv s(y'' + y')(mod\ m) \quad \wedge \quad r(x' - x'') \equiv s(y'' + y')(mod\ n)$$

وهذا يعني حسب تعريف s, r أن :

$$x' \equiv x''\ (mod\ m) \quad \wedge \quad y'' \equiv y'\ (mod\ n)$$

وبالتالي فإن الأعداد z التي عددها $m \cdot n$ تؤلف مجموعة بواقي تامة بالمقاس m ، n فمن أجل كل قيمة لـ e_i : $i = 1, 2, ..., k$ يوجد زوج من الأعداد الصحيحة x_i ، y_i بحيث $e_i \equiv r\,x_i + s\,y_i (mod\ \ mn)$ أي بحيث يكون $e_i \equiv 1 \cdot x_i (mod\ m)$ و $e_i \equiv 1 \cdot y_i (mod\ n)$ وبالتالي نحصل على العلاقة :

$$z + e_i \equiv r(x + x_i) + s(y + y_i)\ (mod\ \ mn)$$

ونعلم أن $z + e_i$ يكون أولياً نسبياً مع $n \cdot m$ إذا وفقط إذا كان أولياً نسبياً مع كل من n, m ويكون z أولياً نسبياً مع m إذا وفقط إذا كان $x + x_i$ أولياً نسبياً مع m ويكون z أولياً نسبياً مع n إذا وفقط إذا كان $y + y_i$ أولياً نسبياً مع n وهذا يعني أن $x + e_i$ أولي نسبياً مع m و $y + e_i$ أولي نسبياً مع n ، ويتم ذلك من أجل جميع قيم e_i حيث $i = 1, 2, ..., k$ بآن واحد وذلك من أجل جميع قيم n التي عددها $\psi(m)$ من المجموعة $1, 2, ..., m$ وجميع قيم y التي عددها $\psi(n)$ من المجموعة $1, 2, ..., n$. مما يدل على أن عدد قيم z التي من أجلها يكون : $(i = 1, 2, ..., k)$ $z + e_i$ أولية نسبياً مع $m \cdot n$ هو $\psi(m)\,\psi(n)$ أي :

$\psi(m.n) = \psi(m) \cdot \psi(n)$ وهو المطلوب .

٢-٣-٢٥ حساب قيمة $\psi(n)$:

١) لنفترض أن $n = p^a$ حيث $a \geq 0$ و p عدد أولي .

ولنرتب القيم من 1 إلى $n = p^a$ على النحو التالي :

1	2	3	....	$p-1$	p
$p+1$	$p+2$	.....	.....	$2p-1$	$2p$
.....	.....	...	....	.....	.....
$(p^{a-1}-1)p+1$	$(p^{a-1}-1)\ p+2$	.....	....	p^{a-1}	p^a

ليكن t عدد البواقي المختلفة بالمقاس p المطابقة بالمقاس p للأعداد $e_1, e_2, \ldots, e_h$ ولتكن هذه البواقي الموجبة هي $r_1, r_2, \ldots, r_t$ عندها نلاحظ أن السطر الأول يحوي t من الأعداد h التي تحقق العلاقات :

$h + r_i \equiv 0 \ (mod\ p)$ $\quad i = 1, 2, \ldots, t$ أي $h \equiv -r_i \ (mod\ p)$ والتي من أجلها $p \mid (h + r_i)$ ويبقى بالتالي في هذا السطر $p - t$ من الأعداد h التي يكون من أجلها $h + r_i \not\equiv 0 \ (mod\ p)$ أي التي تكون أولية نسبياً مع p ، وبالتالي أولية نسبياً مع p^a . من الواضح أن جميع عناصر أي عمود من الأعمدة الموافقة للأعداد h التي عددها $p - t$ والتي يكون من أجلها $h + r_i$ أولياً نسبياً مع p تكون أولية نسبياً مع p (لأنه إذا كان $h + r_i$ أولياً نسبياً مع p فإن $h + r_i + sp$ أولياً نسبياً مع p) وعدد هذه العناصر يساوي p^{a-1} مما يدل على أن عدد الأعداد h التي تحقق الخاصة $h + r_i$ أولية نسبياً مع p مهما تكن $i = 1, 2, \ldots, t$ من بين الأعداد من 1 إلى p^a يساوي $p^{a-1}\ (p-t)$ ، وينتج أن $\psi(p^a) = p^{a-1}\ (p-t)$

وبشكل خاص فإن $\psi(p) = (p-t)$.

٢) حساب $\psi(n)$ حيث $n>1$

نحلل n إلى عوامله الأولية فنكتب $n = p_1^{a_1}\ p_2^{a_2} \dots p_r^{a_r}$ حيث p_i أوليات مختلفة ، لما كانت $\psi(n)$ دالة ضربية فإن :

$$\psi(n) = \psi(p_1^{a_1}) \cdot \psi(p_2^{a_2}) \dots \psi(p_r^{a_r})$$

فإذا كان t_i $(i=1,2,\dots,r)$ هو عدد الأعداد من بين $e_1, e_2, \dots, e_h$ غير المتطابقة بالمقاس p_i أي هو عدد البواقي الموجبة المختلفة للأعداد السابقة بالمقاس p_i فإن :

$$\psi(n) = p_1^{a_1-1}(p_1-t_1)\ p_2^{a_2-1}(p_2-t_2) \dots\dots p_r^{a_r-1}(p_r-t_r)$$

$$= \frac{n}{p_1\ p_2\ \dots\dots p_r}\ (p_1-t_1)(p_2-t_2)\dots\dots(p_r-t_r)$$

$$= n \cdot (1-\frac{t_1}{p_1})(1-\frac{t_2}{p_2})\dots\dots(1-\frac{t_r}{p_r})$$

أمثلة أخرى :

مثال (١) : لنحسب $\psi(5)$ إذا كان $e_1 = 0\ ,\ e_2 = 3\ ,\ e_3 = 8$

الحل : حسب التعريف ثم حسب الدستور السابق

لنبحث عن عدد الأعداد h التي تحقق :

$$(h,5)=1 \qquad (h+3,5)=1 \qquad (h+8,5)=1 \dots\dots *$$

من بين الأعداد $1\ ,\ 2\ ,\dots,5$ فنلاحظ أن الأعداد التي تحقق $(h,5)=1$ هي $1\ ,2\ ,3\ ,4$ ونلاحظ أن :

والمساويات * محققة $(1,5)=1\ ,\ (1+3,5)=1\ ,\ (1+8,5)=1$

المساويات *غير محققة $(2,5)=1\ ,\ (2+3,5)\neq 1$

والمساويات* محققة $(3,5)=1\ ,\ (3+3,5)=1\ ,\ (3+8,5)=1$

والمساويات * محققة $(4,5)=1\ ,\ (4+3,5)=1\ ,\ (4+8,5)=1$

أي أن الأعداد $1\ ,\ 3\ ,\ 4$ تحقق المطلوب وعددها $= 3$ أي $\psi(5) = 3$

وإذا أردنا تطبيق الدستور نلاحظ أن t عدد الأعداد من بين e_1, e_2, e_3 غير المتطابقة بالمقاس 5 هي $t=2$ لأن :

$$e_1 = 0 \quad \text{و} \quad e_2 \equiv e_3 \equiv 3 (mod\, 5)$$

و $\psi(5) = 5 - 2 = 3$

مثال (٢) : احسب $\psi(n)$ باستخدام الدستور علماً أن $n = 45 = 3^2.5$ و $e_1 = 0\,,\ e_2 = 1$

الحل : إن : $\psi(n) = \psi(3^2).\psi(5) = \dfrac{3^2\ (5)}{3\ \ (5)}\ (3-t_1)\,(5-t_2)$

و $t_1 = 2$ (لماذا ؟)

و $t_2 = 2$ أيضاً

وبالتالي :

$$\psi(45) = 3\ (3-2)\,(5-2) = 9$$

مثال (٣) : أوجد باستخدام الدستور $\psi(75)$ من أجل $e_1 = 0\,,\ e_2 = 1\,,\ e_3 = 2$

الحل : لحساب العدد المطلوب $\psi(75)$ من أجل $e_1 = 0\,,\ e_2 = 1\,,\ e_3 = 2$

نكتب : $75 = 3 \times 5^2$ وإن

$$\psi(75) = \psi(3).\psi(5^2) = \frac{3\ .5^2}{3\ \ .5}\ (3-t_1)\,(5-t_2) = 3(3-t_1)\,(5-t_2)$$

ولما كانت $t_1 = 3$ بالتالي $\psi(75) = 0$.

مثال (٤) : أعد المثال (٣) من أجل $n = 77$.

$$\psi(77) = \psi(7).\psi(11) = (7-t_1)\,(11-t_2) = (7-3)\,(11-3) = (4)(8) = 32$$

برر ذلك .

٢-٣-٢٦ الدالتان τ , σ :

- **تعريف :** الدالة τ دالة عددية قيمتها عند n تساوي عدد القواسم الموجبة المختلفة للعدد $n \in Z^+$ ، ومن تعريف الدالة τ يمكن أن نكتب :

$$\tau(n) = \sum_{d|n} 1$$

وعلى سبيل المثال فإن القواسم الموجبة للعدد 12هي :

$1 , 2 , 3 , 4 , 6 , 12$ وعددها $\tau(12) = 6$

مبرهنة : الدالة τ دالة ضربية .

في الحقيقة إن الدالة $f(d) = 1$ أياً كانت $d \geq 1$ دالة ضربية تماماً 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 بـ $F(n) = \sum_{d|n} f(d)$ هي دالة ضربية أي الدالة المعرفة بالمساواة $\tau(n) = \sum_{d|n} 1$ هي دالة ضربية.

٢-٣-٢٧ تعيين الدالة τ :

١) إذا كانت $n = p^a$ حيث p عدد أولي و $a \geq 1$ فإن قواسم n الموجبة هي $1, p, p^2, ..., p^a$ وعددها $a+1$

أي $\tau(p^a) = a + 1$

٢) إذا كانت $n > 1$ و كتبت n بالشكل القانوني أي :

$$n = p_1^{a_1} \; p_2^{a_2} \ldots\ldots p_k^{a_k}$$ فإنّ :

$$\tau(n) = (a_1 + 1)(a_2 + 1) \;\; \ldots\ldots \;\; (a_k + 1)$$

الإثبات : بما أن τ دالة ضربية وبما أن $p_1^{a_1}, p_2^{a_2}, \ldots\ldots, p_k^{a_k}$ أولية نسبياً مثنى مثنى فإنّ :

$$\tau(n) = \tau(p_1^{a_1}) \; \tau(p_2^{a_2}) \ldots\ldots \tau(p_k^{a_k})$$

أي $\tau(n)=(a_1+1)(a_2+1)\ \ldots\ldots\ (a_k+1)$

أمثلة :

١) لنحسب $\tau(p)$ حيث p عدد أولي

$\tau(p)=1+1=2$ وبالتالي : $\tau(5)=\tau(11)=2$

٢) لنحسب $\tau(4)$ و $\tau(63)$

$\tau(4)=\tau(2^2)=2+1=3$ ، $\tau(63)=\tau(3^2.7)=(2+1)(2)=6$

٢-٣-٢٨ : 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 $\sigma(n)$ أنه بالامكان كتابتها على النحو :

$$\sigma(n)=\sum_{d|n} d$$

٢-٣-٢٩ : مبرهنة : الدالة σ هي دالة ضربية .

الإثبات : إن الدالة المعرفة بـ $f(d)=d$ 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 .

٢-٣-٣٠ : حساب $\sigma(n)$:

١) إذا كان $n=p^a$ فإن جميع القواسم الموجبة لـ n هي : $1, p, p^2, \ldots, p^a$ ومجموعها $\sigma(n)=1+p+p^2+\ldots+p^a$

أي $$\sigma(n)=\frac{p^{a+1}-1}{p-1}$$

٢) إذا كان $n>1$ و كتب بالشكل القانوني $n = p_1^{a_1}\ p_2^{a_2} \ldots\ldots\ p_k^{a_k}$

فإن :

$$\sigma(n)=\sigma(p_1^{a_1})\ \sigma(p_1^{a_1})\ldots\ldots\ \sigma(p_k^{a_k})=\frac{p_1^{a_1+1}-1}{p_1-1}\ \ldots\ldots\ \frac{p_k^{a_k+1}-1}{p_k-1}$$

ويمكن كتابة عبارة $\sigma(n)$ كما يلي :

$$\sigma(n)=\prod_{1}^{k}\ \frac{p_i^{a_i+1}-1}{p_i-1}$$

أمثلة :

$\sigma(p)=\dfrac{p^2-1}{p-1}=p+1$ حيث p عدد أولي ومنه :

$$\sigma(5)=6 \quad , \quad \sigma(11)=12 \quad , \quad \sigma(3)=4$$

$$\sigma(180)=\sigma(2^2).\sigma(3^2).\sigma(5)=\frac{2^3-1}{1}.\ \frac{3^3-1}{2}.6=546$$

- **ملاحظة :** إن الدالتين τ , σ ليستا ضربيتين تماماً إذ نلاحظ أن:

$$\tau(20)=\tau(2^2.5)=3\ .\ 2=6$$

في حين $$\tau(2).\tau(10)=2\ .\ 4=8$$

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 $\sigma(2.(10)) = \sigma(20) \neq \sigma(2).\sigma(10)$

٢-٣-٣١ : تمرين هام :

إن جداء القواسم الموجبة لعدد $n > 1$ يساوي $n^{\tau(n)/2}$

الحل : إذا كان d قاسماً ما لـــ n فإن $n = d\ .\ d'$

ولما كان عدد القواسم الموجبة لـــ n يساوي $\tau(n)$ 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 جميـــع 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 (١) : إن مجموعة 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 (٢) : 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 $\sigma(n) = \frac{n}{d_1} + \frac{n}{d_2} + ... + \frac{n}{d_k} = n\left(\frac{1}{d_1} + \frac{1}{d_2} + ... + \frac{1}{d_k}\right)$

أي $\frac{\sigma(n)}{n} = \sum_{d|n} \frac{1}{d}$

مثال (٣) : أوجد العدد الصحيح n الذي يحقق العلاقة :

$$\tau(10\,n) = 10$$

لدينا $10 = 2 \,.\, 5$ فهو جداء عددين أوليين فقط لذا فإن $10\,n$ يلزم أن تكون من الشكل $10\,n = 2^a.5^b$ وعندها يكون

$$\tau(10\,n) = (a+1)\,(b+1) = 10$$

ومنه نجد أنه إما $a+1 = 2$, $b+1 = 5$ أي $a = 1$, $b = 4$

ومنه فإن $10\,n = 2.5^4$ ومنه $n = 5^3 = 125$

و إما $a+1 = 5$, $b+1 = 2$ أي $a - 4$, $b = 1$

و $10\,n = 2^4.5$ أي $n = 2^3 = 8$

٢-٣-٣٢ : 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 $\sigma(6)=\sigma(2).\sigma(3)$

$\sigma(6)=\frac{2^2-1}{2-1}\ \frac{3^2-1}{3-1}=\frac{3(8)}{2}=12$ أي $\sigma(6)=12=(2)(6)$

والعدد $n=28$ حيث $\sigma(28)=\sigma(2^2).\sigma(7)=(7)(8)=56=(2)(28)$

• ونقول إن العدد الصحيح n فوق الكامل(عدد زائد) 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 (عدد ناقص) إذا كان $\sigma(n)<2n$.

مثال ذلك العدد 8 إذ إنّ : $\sigma(8)=\sigma(2^3)=15<(2)(8)$

• نقول إن العددين m,n عددان متحابان إذا كان :

$$\sigma(n)=\sigma(m)=n+m$$

أو إذا كان $\sigma(m)-m=n \quad \wedge \quad \sigma(n)-n=m$

مثال ذلك : 284 و 220

وقد وجد العلماء عدداً من الأعداد الكاملة وكلها زوجية ، هل يوجد عدد كامل فردي ؟ مسألة مفتوحة ، هل يوجد عدد غير منته من الأعداد الكاملة ؟ لقد وُجِد أن العدد الخامس هو $p_5=33.550336$ وأن العدد السادس مؤلف من عشرة أرقام مما يدل على ندرة هذه الأعداد . ولم يعرف حتى عام 1968 سوى 23 عدداً كاملاً وكلها زوجية ، وقد تبين أنه إن وجد عدد كامل فردي فهو أكبر حتماً من العدد 10^{200}.

إن مسألة البحث عن صيغة للأعداد الكاملة مسألة قديمة وقد أثبت اقليدس أنه إذا كان المجموع $1+2+2^2+.....+2^{k-1}=p$ عدداً أولياً فإن العدد $2^{k-1}.p$ هو عدد كامل وعلى سبيل المثال إن : $1+2+4=7$ هو عدد أولي و $(7)(4)=28$ هو عدد كامل ، وقد أثبت أولر بعد 2000 سنة أن جميع الأعداد الكاملة الزوجية لها هذا الشكل الأمر الذي سنوضحه في المبرهنة التالية:

٢-٣-٣٣ 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 حصراً 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

$$\sigma(n)=2\,n=2^k q$$

والعلاقة $2^k q=(2^k-1)\,\sigma(q)$ تدل على أن $2^k-1\,|\,2^k.q$

ولما كان $(2^k-1,2^k)=1$ فإن : $2^k-1\,|\,q$

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 $M < q$ فـإن : $\sigma(q) \geq q + M$

ولكن : $q + M = 2^k M$ أي أن $\sigma(q) = q + M$ مما يدل علـى أن للعـدد قاسمان فقط هما M و q ينتج من ذلـك أن q عـدد أولـي وأن $M = 1$.

نعوض في قيمة q لنجد أخيراً أن : $q = 2^k - 1$ وهو المطلوب .

٢-٣-٣٤ 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 $a^k - 1$ يجـب 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 قيمـة كـل مـن العاملين في الطرف الثاني أكبر من الواحد وهذا يناقض كـون $a^k - 1$ عـدداً أولياً مما يثبت أن k لا بد وأن يكون أولياً .

- **ملاحظة :** نلاحظ أنه من أجل $p = 2$ أن $2^2 - 1 = 3$ عدد أولي

والعدد $2\,(2^2 - 1) = 6$ عدد كامل

ومن أجل $p = 3$ فإن $2^3 - 1 = 7$ عدد أولي والعدد $2^2\,(2^3 - 1) = 28$ عدد كامل

ومن أجل $p = 5$ فإن $2^5 - 1 = 31$ عدد أولي والعدد $2^4\,(2^5 - 1) = 496$ عدد كامل

ظن الرياضيون القدماء أن الصيغة $2^p - 1$ تعطي دائماً 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 التي من الشكل $M_p = 2^p - 1$ 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 أولر عام 1772 من أن M_{31} عدد أولي . ثم أثبت لوقا عام 1876 أن M_{67} عدد مؤلف ، مخالفا لتوقع ميرسن ، ولكن دون أن يعين عوامله الأولية التي عينها بعد ذلك الرياضي الأمريكي فريدريك نلسون كول عام 1903 .

* انظر جدول أعداد ميرسن في الملحق(٤)والموقع المرافق لها على الانترنيت.

٢-٣-٣٥ دالة موبياس *Mobius - function* :

تعريف : نعرف الدالة μ عند أي عدد صحيح موجب n كما يلي :

$$\mu(n) = \begin{cases} 1 & \text{عندما } n = 1 \\ 0 & \text{إذا وجد عدد أولي } p \text{ بحيث } p^2 \mid n \\ (-1)^r & \text{إذاكان } n = p_1 p_2 \ldots p_r \text{ و } p_i \text{ أوليات مختلفة} \end{cases}$$

من التعريف ينتج أن $\mu(1) = 1$, $\mu(2) = -1$, $\mu(3) = -1$

$\mu(4) = 0$, $\mu(5) = -1$, $\mu(6) = 1$, $\mu(50) = 0$

لاحظ أن :

$\mu(p) = -1$ دائماً عندما p عدد أولي

$\mu(p^k) = 0$ من أجل p عدد أولي و $k \geq 2$

٢-٣-٣٦ مبرهنة: إن دالة موبياس هي دالة 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 $m=p_1p_2...p_r$ وأن $n=q_1q_2...q_s$

حيث p_i ، q_j أوليات مختلفة . فعندها نكتب

$$\mu(m\,.\,n)=\mu(\,p_1p_2...p_r\;\;q_1q_2...q_s\,)=(-1)^{r+s}=(-1)^r(-1)^s=\mu(m)\mu(n)$$

٢-٣-٣٧ مبرهنة : من أجل أي عدد صحيح $n\geq 1$ فإن :

$$G(n)=\sum_{d|n}\mu(d)=\begin{cases}1 & n=1 \quad \text{عندما}\\ 0 & n>1 \quad \text{عندما}\end{cases}$$

الإثبات : نلاحظ أن $\sum_{d|1}\mu(d)=\mu(1)=1$

لنفترض أن $n>1$ ولنحسب $G(\,n\,)$

١) إذا كان $n=p^k$ نكتب :

$$G(n)=G(p^k)=\sum_{d|n}\mu(d)=\mu(1)+\mu(p)+\mu(p^2)+....+\mu(p^k)$$

$$G(p^k)=\mu(1)+\mu(p)=1+(-1)=0$$

٢) إذا كان $n=p_1^{k_1}\;p_2^{k_2}\;.....\;p_r^{k_r}$ فإن

$$G(n)=G(p_1^{k_1}\;p_2^{k_2}\;.....\;p_r^{k_r})=G(\,p_1^{k_1})\,.\,G(\,p_2^{k_2})\;.....G(\,p_r^{k_r})$$

ولما كانت الدالة μ ضربية فإن G دالة ضربية

وينتج من ذلك أن : $G(n)=0$

مثال : لتكن $n=10$ ، إن قواسم n هي $1\,,2\,,5\,,10$

ومنه

$$G(10)=\sum_{d|10}\mu(d)=\mu(1)+\mu(2)+\mu(5)+\mu(10)$$
$$=1+(-1)+(-1)+1=0$$

٢-٣-٣٨ صيغة موبياس للتعاكس : (*Mobius inversion formula*)

إذا كانت : $f\,,\,F$ دالتين عدديتين (حسابيتين) 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 : نلاحظ أولاً أن الدالة f تتعين بشكل وحيد بدلالة F 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 :

$$*\quad \sum_{d|n}\mu(d)\,F(\frac{n}{d})=\sum_{d|n}\mu(d)\sum_{m|\frac{n}{d}}f(m)=\sum_{d|n}\sum_{m|\frac{n}{d}}\mu(d)\,f(m)$$

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 ٢-٣-٣٧ 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 أنه 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

$$\sum_{d|10} \sum_{m|\frac{10}{d}} \mu(d)\ f(m) = \mu(1)\ [f(1) + f(2) + f(5) + f(10)] +$$

$$\mu(2)\ [f(1) + f(5)] + \mu(5)\ [f(1) + f(2)] + \mu(10)\ f(1)$$

$$= f(1)\ [\mu(1) + \mu(2) + \mu(5) + \mu(10)] + f(2)\ [\mu(1) + \mu(5)] +$$

$$+ f(5)\ [\mu(1) + \mu(2)] + f(10)\,\mu(1) = \sum_{m|10} \sum_{d|\frac{10}{m}} f(m)\ \mu(d)$$

٢-٣-٣٩ تطبيقات

١- نعلم أن $\tau(n)=\sum_{d|n} 1$ و $\sigma(n)=\sum_{d|n} d$

باستخدام صيغة موبياس للتعاكس نجد أن

$$n=\sum_{d|n}\mu(\frac{n}{d})\,\sigma(d) \quad \text{و} \quad 1=\sum_{d|n}\mu(\frac{n}{d})\,\tau(d)$$

عندما $n\geq 1$

٢-٣-٤٠ مبرهنة : إذا كانت F, f دالتين عدديتين وكان

$$F(n)=\sum_{d|n} f(d)$$

وإذا كانت F دالة ضربية فإن f دالة ضربية .

البرهان : نلاحظ أولاً أن $F(1)=f(1)=1$

ثم لنكتب عبارة $f(n)$ وفق صيغة موبياس للتعاكس :

$$f(n)=\sum_{d|n}\mu(d)\,F(\frac{n}{d})$$

ولنأخذ العددين n و m بحيث يكون $(m,n)=1$ ونكتب :

$$f(m.n)=\sum_{d|m.n}\mu(d)\,F(\frac{m\,n}{d})$$

نعلم أن أي قاسم d للجداء $m.n$ يمكن أن يكتب على النحو $d=d_1\,d_2$

حيث $d_1|m \wedge d_2|n$ و $(d_1,d_2)=1$ لأن $(m,n)=1$

وتصبح عبارة $f(m.n)$ بالتالي على النحو :

$$f(m.n)=\sum_{\substack{d_1|m\\ d_2|n}}\mu(d_1d_2)\,F(\frac{m}{d_1}.\frac{n}{d_2})$$

ولدينا $\mu(d_1 . d_2) = \mu(d_1)\mu(d_2)$ و $F(\frac{m}{d_1}.\frac{n}{d_2}) = F(\frac{m}{d_1}) . F(\frac{n}{d_2})$

لأن μ و F دالتان ضربيتان الأمر الذي يعطي

$$f(m.n) = \sum_{\substack{d_1 | m \\ d_2 | n}} \mu(d_1) F(\frac{m}{d_1}) \mu(d_2) F(\frac{n}{d_2})$$

ومنه :

$$f(m.n) = \sum_{d_1 | m} \mu(d_1) F(\frac{m}{d_1}) \sum_{d_2 | n} \mu(d_2) F(\frac{n}{d_2})$$

$$= f(m).f(n)$$

تمرين : عين الدالة g علماً أن $\sum_{d|n} g(d) = n \quad , \quad n \geq 1$

الحل : نكتب عبارة $g(n)$ حسب صيغة موبياس للتعاكس حيث $F(n) = n$ فنجد:

$$g(n) = \sum_{d|n} \mu(d) . \frac{n}{d}$$

ونلاحظ أنه إذا كان $n = 1$ فإن $g(1) = 1$.

وإذا كان $n = p^\alpha$ حيث p عدد أولي فإن :

$$g(p^\alpha) = \mu(1) p^\alpha + \mu(p) p^{\alpha-1} + ... + \mu(p^\alpha).1$$

$$g(n) = g(p^\alpha) = p^\alpha - p^{\alpha-1}$$

وإذا كان $n = p_1^{\alpha_1} ..... p_r^{\alpha_r}$ فإن:

$$g(n) = g(p_1^{\alpha_1}) g(p_2^{\alpha_2}) ..... g(p_r^{\alpha_r})$$

$$= \prod_{i=1}^{r} p_i^{\alpha_i - 1}(p_i - 1)$$

وهذه الصيغة هي قيمة دالة أولر كما مر معنا أي :

$$g(n) = \varphi(n)$$

إن هذه النتيجة تثبت ثانية أن :

$$\sum_{d|n} \varphi(n) = n$$

ونهاية هذا الفصل سنورد تعريفاً لدالتين عدديتين دون التعرض لخواصهما

تعريف (١) : دالة ليوفيل λ (*Liouville's Function*)

نعرف دالة ليوفيل كما يلي :

$$\lambda(n) = \begin{cases} 1 & \text{عندما } n = 1 \\ (-1)^{\alpha_1+\alpha_2+\dots+\alpha_r} & \text{عندما } n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_r^{\alpha_r} \end{cases}$$

إذاً $\lambda(1) = 1 \quad , \quad \lambda(2) = \lambda(3) = \lambda(5) = 1$

مما يدل على أن

$$\lambda(4) = \lambda(6) = 1 \quad , \quad \lambda(7) = \lambda(8) = -1 \quad , \quad \lambda(9) = \lambda(10) = 1$$

ويلاحظ مباشرة من التعريف أنها دالة ضربية .

تعريف (٢) : دالة مانجولد $\wedge$ (*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

$$(1) \qquad \sum_{d|n} \wedge(d) = \log n$$

$$(2) \qquad \wedge(n) = \sum_{d|n} \mu(n/d) \log d$$

تمارين

١) أثبت أنه إذا كان $\alpha , \beta \in \Re$ فإن :

1) $[4\alpha]+[4\beta] \geq 2[\alpha]+2[\beta]+2[\alpha+\beta]$

2) $[4\alpha]+[4\beta] \geq 3[\alpha]+3[\beta]+[\alpha+\beta]$

3) $[3\alpha]+[3\beta] \geq [\alpha]+[\beta]+2[\alpha+\beta]$

٢) إذا كان n , m عددين صحيحين فأثبت أن :

1) $\dfrac{(4m)!\,(4n)!}{(m!)^2(n!)^2[(m+n)!]^2}$ هو عدد صحيح

2) $\dfrac{(4m)!\,(4n)!}{(m!)^3(n!)^3(m+n)!}$ هو عدد صحيح

3) $\dfrac{(3m)!\,(3n)!}{m!\,n!\,[(m+n)!]^2}$ هو عدد صحيح

٣) أثبت أن أس اكبر قوة للعدد 7 تقسم $(7^n-3)!$ هي $(7^n-6n-1)/6$

٤) أثبت أن أس اكبر قوة للعدد 5 تقسم $(5^n-4)!$ هي $(5^n-4n-1)/4$

٥) أوجد أس أكبر قوة للعدد 3 تقسم $80!$.

٦) أوجد أس أكبر قوة للعدد 7 تقسم $2400!$.

٧) إذا كان n عدداً صحيحاً موجباً فأثبت أن :

$$\mu(n)\,\mu(n+1)\,\mu(n+2)\,\mu(n+3)=0$$

٨) إذا كان $n \geq 3$ أثبت أن $\sum_{k=1}^{n} \mu(k!) = 1$.

٩) 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) $\sum_{d|n} d\,.\,\mu(d) = (1 - p_1)(1 - p_2) \dots\dots (1 - p_r)$

١٠) إذا كان $\lambda(n)$ دالة ليوفيل و $n > 0$ فأثبت أن :

$$\sum_{d|n} \lambda(d) = \begin{cases} 1 & \text{إذا وجد عدد صحيح } m \text{ بحيث } n = m^2 \\ 0 & \text{فيما عدا ذلك} \end{cases}$$

١١) إذا كان $(a, 30) = 1$ أثبت أن $240 \mid a^4 - 1$.

١٢) إذا كان $n \geq 0$ أثبت أن $240 \mid f(n)$ حيث

$$f(n) = 6\,.\,17^{4n} - 5\,.\,13^{4n^2} - 1$$

١٣) إذا كان a عدداً فردياً و $(a, 3) = 1$ أثبت أن :

$$192 \mid a^4 + 14a^2 - 96a + 81$$

١٤) أثبت أن $\tau(n)$ يكون عدداً فردياً إذا وفقط إذا كان n مربعاً كاملاً .

١٥) أثبت أن $\sigma(n)$ يكون عدداً فردياً إذا وفقط إذا كان $n = m^2$ أو $n = 2m^2$ من أجل عدد ما m .

١٦) أوجد صيغة n حتى يكون $\tau(n) = 10$ ، هل يوجد عدد n يحقق العلاقة : $\sigma(n) = 10$ ؟

١٧) إذا كان $k \geq 0$ أثبت ما يلي :

$$n = 2^{k-1} \Rightarrow \sigma(n) = 2n - 1$$

١٨) احسب : ١) $\psi(3025)$ علماً أن $e_1 = 1 \ , \ e_2 = 4 \ , \ e_3 = 7$

٢) $\psi(50)$ علماً أن $e_1 = 0 \ , \ e_2 = 3 \ , \ e_3 = 4$

٣) $\psi(168)$ علماً أن $e_1 = 0 \ , \ e_2 = 1 \ , \ e_3 = 9$

١٩) أثبت أن قوة عدد أولي لا يمكن أن يكون عدداً كاملاً .

٢٠) أثبت أن n^2 لا يمكن أن يكون عدداً كاملاً .

٢١) جداء أي عددين أوليين فرديين ليس عدداً كاملاً .

٢٢) إذا كان n عدداً كاملاً أثبت أن $\sum_{d|n} \frac{1}{d} = 2$

٢٣) من أجل أي عدد كامل زوجي $n > 6$ أثبت أن مجموع أرقام n يطابق الواحد بالمقاس 9 .

٢٤) أثبت أنه لا يمكن لأي قاسم لعدد كامل أن يكون كاملاً .

٢٥) استخدم مبرهنة أولر 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

٢٦) أثبت أنه إذا كان $(a, n) = (a-1, n) = 1$ فإن :

$$1 + a + a^2 + \ldots\ldots + a^{\varphi(n)-1} \equiv 0 \ (mod\ n)$$

٢٧) إذا كان $(m, n) = 1$ حيث n و m عددان صحيحان موجبان فأثبت أن $m^{\varphi(n)} + n^{\varphi(m)} \equiv 1 \ (mod\ mn)$

٢٨) أثبت أن المجموعة $\{3, 3^2, 3^3, 3^4, 3^5, 3^6\}$ هي مجموعة بواق مختزلة بالمقاس 14 .

٢٩) أثبت أن المجموعة $\{2, 2^2, 2^3, \ldots, 2^{16}\}$ هي مجموعة بواق مختزلة بالمقاس 27 .

٣٠) إذا كان $n>1$ لا يحوي عوامل أولية مكررة فأثبت أن $\tau(n^2)=n$ إذا وفقط إذا كان $n=3$.

٣١) أثبت أن $3|\sigma(3n+2)$ و $4|\sigma(4n+3)$ من أجل أي عدد صحيح موجب n .

الفصل الرابع والأخير

الجذور الأولية والأدلة

المرتبة

الجذور الأولية

الدليل وخواص الأدلة

حل التطابقات الخطية باستخدام الأدلة

٤-١ المرتبة

٤-١-١ تعريف المرتبة : إن مرتبة أو رتبة العدد a بالمقاس m (أو الأس الذي ينتمي إليه العدد الصحيح a بالمقاس m) حيث $(a, m) = 1$ هو أصغر عدد صحيح موجب $e \neq 0$ يحقق العلاقة $a^e \equiv 1 \pmod{m}$ ، ونقول إن e هو دليل أولر (أو دليل) للعدد a بالمقاس m ونكتب $e = \operatorname{Ind} a \pmod{m}$

أمثلة :

- مرتبة العدد 2 بالمقاس 7 هي 3 ذلك أن :

$$2^1 \equiv 2 \pmod{7} \quad , \quad 2^2 \equiv 4 \pmod{7} \quad , \quad 2^3 \equiv 1 \pmod{7}$$

- مرتبة العدد 5 بالمقاس 6 هي 2 ذلك أن :

$$5^2 \equiv 1 \pmod{6}$$

لذا نقول إن 2 هو دليل العدد 5 بالمقاس 6 .

- مرتبة العدد 3 بالمقاس 14 هي 6 ذلك أن :

$$3^1 \equiv 3 \bmod 14$$
$$3^2 = 9 \bmod 14$$
$$3^3 \equiv -1 \bmod 14$$
$$3^4 \equiv 11 \bmod 14$$
$$3^5 \equiv 5 \bmod 14$$
$$3^6 \equiv 1 \bmod 14$$

٤-١-٢ مبرهنة :

إذا كانت مرتبة العدد الصحيح a تساوي e بالمقاس m فإن: $a^k \equiv 1 \pmod{m}$ إذا وفقط إذا كان $e \mid k$ (أي إذا كان k مضاعفاً لـ e).

الإثبات : إذا كان $e \mid k$ فإن $k = ee_1$ وبالتالي:

$$a^k = (a^e)^{e_1} \equiv (1)^{e_1} \equiv 1 \pmod{m}$$

وبالعكس إذا كان k عدداً صحيحاً موجباً يحقق العلاقة $a^k \equiv 1 \pmod{m}$

فحسب خوارزمية القسمة نكتب $k = eq + r \qquad 0 \le r < e$

$$a^k \equiv (a^e)^q \cdot a^r \pmod{m}$$

ولما كان كل من a^k و a^e يطابق الواحد بالمقاس m فإن العلاقة الأخيرة تعطي $a^r \equiv 1 \pmod{m}$ ولكن حسب تعريف المرتبة فإن e هي أصغر عدد صحيح موجب يحقق التطابق السابق و $0 \le r < e$

إذاً $r = 0 \quad , \quad k = eq$ أي $e \mid k$

- **نتيجة** : نعلم من مبرهنة أولر أن $a^{\varphi(m)} \equiv 1 \pmod{m}$

ومما يدل على أنه إذا كانت e مرتبة a بالمقاس m فإن e يجب أن تقسم $\varphi(m)$ وبالتالي يكفي أن تبحث عن مرتبة العدد a بالمقاس m بين قواسم $\varphi(m)$. {تذكر : ترمز $\varphi(m)$ إلى عدد الأعداد الموجبة التي تصغر m والأولية نسبياً مع m }

فعلى سبيل المثال إذا أردنا البحث عن مرتبة العدد 2 بالمقاس 13 نحسب $\varphi(13) = 12$ ثم نبحث عن المرتبة بين قواسم العدد 12 أي بين الأعداد $1, 2, 3, 4, 6, 12$ وهنا نرى أن

$$2^2 \equiv 4 \ , \ 2^3 \equiv 8 \ , \ 2^4 \equiv 3 \ , \ 2^6 \equiv 12 \ , \ 2^{12} \equiv 1 \pmod{13}$$

إذن مرتبة العدد 2 بالمقاس 13 هي 12

- **تمرين** :

هل يوجد عدد a مرتبته تساوي $\varphi(12)$ بالمقاس 12 ؟ أي هل للمعادلة $a^4 \equiv 1 \bmod 12$ حل؟

نعلم من التعريف أن العدد a إن وجد يجب أن يكون أولياً نسبياً مع 12 ويصغره لذا سنبحث عن العدد a ضمن مجموعة البواقي المختزلة للعدد 12 أي ضمن المجموعة $\{1,5,7,11\}$ وهنا نرى أن:

$$1^2 = 5^2 = 7^2 = 11^2 \equiv 1 \ (mod 12)$$

إذن الجواب : لا يوجد للمعادلة المعطاة حل.

٤-١-٣ مبرهنة : إذا كانت مرتبة a بالمقاس m هي e فإن

$a^t \equiv a^s \ (mod\ m)$ إذا وفقط إذا كان $t \equiv s \ (mod\ e)$

الإثبات : لنفترض أولاً أن $a^t \equiv a^s \ (mod\ m)$ حيث $t \geq s$

نعلم أن $(a, m) = 1$ لذا يمكن اختصار a^s من الطرفين لنجد :

$$a^{t-s} \equiv 1 (mod\ m)$$

وحسب ما سبق فإن $e \mid t-s$ أي $t \equiv s \ (mod\ e)$

وبالعكس إذا كان $t \equiv s \ (mod\ e)$ لأمكننا أن نكتب :

$t = s + qe$ ولدينا $a^e \equiv 1 \ (mod\ m)$ أي

$$a^t \equiv a^s . (a^e)^q \equiv a^{s+qe} \equiv a^s \ (mod\ m)$$

- **نتيجة :** إذا كانت مرتبة a بالمقاس m هي e فإن الأعداد

$a, a^2, \ldots\ldots, a^e$ غير متطابقة بالمقاس m

البرهان : لو كان $a^t \equiv a^s \ (mod\ m)$ حيث $1 \leq t \leq s \leq e$

فإن المبرهنة السابقة تؤكد أن $t \equiv s \ (mod\ e)$ وهذا غير ممكن من أجل القوى المختلفة لـ a السابقة .

٤-١-٤ مبرهنة : إذا كانت مرتبة العدد a بالمقاس m تساوي e وكان $k > 0$ فإن مرتبة a^k بالمقاس m هي $\frac{e}{d}$ حيث $d = (k, e)$

الإثبات : لما كان $d = (k, e)$ فإن : $k = k_0 d$, $e = e_0 d$, $(k_0, e_0) = 1$

فإذا افترضنا أن r هي مرتبة a^k بالمقاس m لكان :

$$(a^k)^r \equiv a^{kr} \equiv 1 (mod\ m) \Rightarrow e \mid kr \Rightarrow e_0 \mid k_0 r$$

ولما كان $(k_0, e_0) = 1$ ينتج أن $e_0 \mid r$ (١)

ومن جهة أخرى نكتب :

$$(a^e)^{k_0} \equiv a^{ek_0} \equiv a^{edk_0} \equiv (a^k)^{e_0} \equiv 1 (mod\ m)$$

ولما كانت r هي مرتبة a^k بالمقاس m فإن $r | e_0$ (٢)

ومن العلاقتين (١) و(٢) ينتج أن $r = e_0 = \frac{e}{d}$

– **نتيجة :** إذا كان $(k,e)=1$ فإن مرتبة a^k تساوي مرتبة a بالمقاس m

تمرين هام : عين مراتب الأعداد من 1 إلى 12 بالمقاس 13

الحل : بالاعتماد على المبرهنات السابقة يمكن أن نرتب الجدول التالي :

العدد : a	1	2	3	4	5	6	7	8	9	10	11	12
المرتبة : e	1	12	3	6	4	12	12	4	3	6	12	2

يلاحظ من الجدول أن مرتبة العدد 2 بالمقاس 13 تساوي 12 ومرتبة العدد $2^2 = 4$ تساوي $\frac{12}{2} = 6$ ومرتبة العدد $2^3 = 8$ تساوي $\frac{12}{3} = 4$ ومرتبة العدد $2^4 \equiv 3 (mod\ 13)$ تساوي $\frac{12}{4} = 3$ ومرتبة العدد $2^5 \equiv 6 (mod\ 13)$ تساوي 12 لأن $(5,12)=1$ ومرتبة العدد $2^6 \equiv 12 (mod\ 13)$ تساوي $\frac{12}{6} = 2$ لأن $(6,12)=6$ ومرتبة العدد $2^7 \equiv 11 (mod\ 13)$ تساوي 12 لأن $(7,12)=1$ ومرتبة العدد $2^8 \equiv 9 (mod\ 13)$ تساوي $\frac{12}{4} = 3$

ويمكن أن نكتب : $3^2 = 9$, $(2,3)=1$ فمرتبة 9 تساوي مرتبة 3 بالمقاس 13 أي تساوي 3

ومرتبة $2^9 \equiv 5 (mod\ 13)$ تساوي $\frac{12}{(9,12)} = 4$

ومرتبة $2^{10} \equiv 10 (mod\ 13)$ تساوي $\frac{12}{(10,12)} = 6$

ومرتبة $2^{11} \equiv 7 (mod\ 13)$ تساوي $\frac{12}{(11,12)} = 12$

٤-١-٥ مبرهنة :

إذا كانت e مرتبة العدد a بالمقاس m وكانت f مرتبة العدد b 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 $(a.b)^k \equiv 1 (mod\ m)$ وبرفع الطرفين إلى القوة e نجد :

$$((ab)^k)^e \equiv (a^e)^k b^{ke} \equiv b^{ke} \equiv 1 (mod\ m)$$

ولما كانت مرتبة b هي f فإن $f \mid ke$ ولكن $(f, e)=1$ الأمر الذي يعطي $f \mid k$

وبمناقشة مماثلة يمكن أن نكتب :

$$((ab)^k)^f \equiv a^{kf} . (b^f)^k \equiv a^{kf} \equiv 1 (mod\ m)$$

ولما كانت مرتبة a بالمقاس m هي e فإن $e \mid kf$ و $(f, e)=1$ أي $e \mid k$ وبالتالي فإن $e.f \mid k$ (١)

ومن جهة أخرى نجد أن $(ab)^{e.f} \equiv (a^e)^f . (b^f)^e \equiv 1 (mod\ m)$

ولما كانت مرتبة $a . b$ هي k فإن $k \mid e.f$ (٢)

من العلاقتين (١) و (٢) نجد أن $k = e.f$

تطبيق: نلاحظ أن مرتبة العدد 2 بالمقاس 7 تساوي 3 ومرتبة العدد 6 بالمقاس 7 تساوي 2 و $(2,3)=1$ ، وبالتالي فإن مرتبة العدد الناتج عن حاصل ضربهما: $2.6=12\equiv 5(mod\ 7)$ بالمقاس7 تساوي $3\ .\ 2 = 6$ أي :

$$5^6 \equiv 1(mod\ 7)$$

والعدد 6 هو أصغر عدد يحقق هذا التطابق(تحقق من ذلك!)

٤-٢ الجذور الأولية « ***Primitive roots*** »

٤-٢-١ تعريف الجذر الأولي : إذا كان $(a, m)=1$ وكانت مرتبة a بالمقاس m تساوي $\varphi(m)$ فإن a يسمى جذراً أولياً (أو جذراً أصلياً) للعدد m .

أي إذا كان العدد $\varphi(m)$ يساوي أصغر أو أول عدد صحيح موجب يحقق العلاقة $a^{\varphi(m)}\equiv 1(mod\ m)$ وكان $(a, m)=1$ فإن a هو جذر أولي (أصلي) للعدد m .

يمكن أن يكون لعدد ما عدة جذور أولية (أصلية) بالمقاس m وقد لا يوجد لعدد ما أي جذر أولي .

مثال : رأينا سابقاً أن مرتبة كل عدد من الأعداد $\{2, 6, 7, 11\}$ بالمقاس 13 تساوي $\varphi(13)=12$ فللعدد 13 أربعة جذور أولية (أصلية) بكلمات أخرى للمعادلة $a^{12}\equiv 1 mod 13$ 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 بكلمات أخرى ليس للمعادلة $a^4\equiv 1 mod 12$ أي حل.

٤-٢-٢ مبرهنة : إذا كان $(a, m)=1$ وإذا كان a جذراً أولياً للعدد m فإن مجموعة الأعداد $\{a, a^2, \ldots, a^{\varphi(m)}\}$ هي بواق مختزلة بالمقاس m.

الإثبات : بما أن a جذر أولي لـــ m فإن $a^{\varphi(m)} \equiv 1 (mod\ m)$ وحسب نتيجة المبرهنة ٤-٢-٣ فإن الأعداد التالية التي عددها $\varphi(m)$:

$a , a^2 , ... , a^{\varphi(m)}$ غير متطابقة بالمقاس m

ولدينا من جهة ثانية $(a, m)=1$ مما يدل على أن قوى a هي أولية نسبياً أي أن المجموعة $T_m = \{ a , a^2 , ... , a^{\varphi(m)} \}$ هي مجموعـــة بـــواق مختزلـــة بالمقاس m .

٤-٢-٣ **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 $(a, m)=1$ ومرتبـــة العدد a تساوي $\varphi(m)$ بالمقاس m . إن أي جذر أولي لـــ m يجب أن يكـــون أولياً نسبياً مع m فهو أحد عناصر مجموعة البواقي المختزلة بالمقاس m أي هو أحد عناصر المجموعة $T_m = \{ a , a^2 , ... , a^{\varphi(m)} \}$. ونعلم أن مرتبة a^k بالمقاس m تساوي مرتبة a بالمقاس m إذا كان $(\varphi(m), k)=1$ أي أن عدد العناصر التي مرتبتها = $\varphi(m)$ من المجموعة $T(m)$ (أي عدد الجـــذور 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 لـــ p أي إذا كانت مرتبة r هي $\varphi(p) = p-1$ فإن عدد الجذور الأوليـــة للعـــدد p يـــساوي $\varphi(p-1)$ ، وعلى سبيل المثال إذا كان $p= 7$ فـــإن $\varphi(7) = 6$ و $\varphi(6) = 2$ فللعدد 7 جذران أوليان (أصليان) هما 3 و 5 ذلك أن أس أصغر قوة للعـــدد 3 يحقق التطابق $3^e \equiv 1 (mod\ 7)$ هو 6 أي أن العدد 3 هو جذر أولي للعدد 7

كذلك نرى أن $5^6 \equiv 1(\bmod 7)$ و 6 هو مرتبة العدد 5 بالمقاس 7 (انظر صفحة ١٧٤).

سنورد فيما يلي المبرهنة الهامة التالية دون سرد لإثباتها .

٤-٢-٤ مبرهنة: يوجد للعدد m جذر أولي إذا وفقط إذا كان $m=2$ أو $m=4$ أو كان من الشكل $m=p^n$ أو $m=2p^n$ حيث p عدد أولي فردي و n عدد صحيح موجب .

تمرين : أوجد الجذور الأولية للعدد $3^2=9$.

الحل : إن مجموعة البواقي المختزلة للعدد 9 هي :

$$T(9)=\{1,2,4,5,7,8\}$$

والجذور الأولية إن وجدت هي قوى عناصر المجموعة $T(9)$. ونلاحظ أن

$$2^2=4\ ,\ 2^3=8\ ,\ 2^4\equiv 7(mod\ 9),\ 2^5\equiv 5(mod\ 9),\ 2^6\equiv 1(mod\ 9)$$

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 $k=5$, $2^5\equiv 5(mod\ 9)$ والعدد 5 هو الجذر الأولي الثاني . في الحقيقة فإن

$$2^5\not\equiv 1(mod\ 9)\ ,\ 5^3\equiv -1(mod\ 9)\ \Rightarrow\ 5^6\equiv 1(mod\ 9)$$

٤-٣ الأدلة Indices

٤-٣-١ 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 $b\equiv r^k(mod\ m)$ يسمى دليل أولر للعدد b أو لغاريتم أولر للعدد b

أو دليل b اختصاراً بالأساس r والمقاس m ونكتب

$$k = \underset{r}{\mathrm{Ind}}\, b \quad \Leftrightarrow \quad r^{\mathrm{Ind}\, b} \equiv b \,(mod\ m)$$

مثال : بما أن $r = 2$ جذر أولي للعدد 5 و $\varphi(5) = 4$ وأن قوى العدد 2 هي :

$$2^1 \equiv 2(mod\ 5),\ \ 2^2 \equiv 4(mod\ 5)\ ,\ 2^3 \equiv 3(mod\ 5)\ ,\ 2^4 \equiv 1(mod\ 5)$$

لذا نقول إن $\underset{2}{\mathrm{Ind}}\, 2 = 1\ ,\ \underset{2}{\mathrm{Ind}}\, 4 = 2\ ,\ \underset{2}{\mathrm{Ind}}\, 3 = 3\ ,\ \underset{2}{\mathrm{Ind}}\, 1 = 4$

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 .

٤-٣-٢ خواص الأدلة : إذا كان r جذراً أولياً للعدد m وإذا كان N و M عددين صحيحين وكان $(M.N, m) = 1$ فإن

١) $$\underset{r}{\mathrm{Ind}}\, M = \underset{r}{\mathrm{Ind}}\, N(mod\ \varphi(m)) \quad \Leftrightarrow \quad M \equiv N\,(mod\ m)$$

البرهان : من تعريف الأدلة نكتب

$$M = r^{\mathrm{Ind}\, M}\,(mod\ m) \quad \wedge \quad N = r^{\mathrm{Ind}\, N}\,(mod\ m)$$

$$M \equiv N\,(mod\ m) \Leftrightarrow r^{\mathrm{Ind}\, M} \equiv r^{\mathrm{Ind}\, N}\,(mod\ m)$$

وحسب المبرهنة ٤-٢-٣ فإن :

$$r^{\mathrm{Ind}\, M} \equiv r^{\mathrm{Ind}\, N}\,(mod\ m) \Leftrightarrow \underset{r}{\mathrm{Ind}}\, M \equiv \underset{r}{\mathrm{Ind}}\, N(mod\ \varphi(m))$$

٢) $$\underset{r}{\mathrm{Ind}}\, M.N \equiv (\underset{r}{\mathrm{Ind}}\, M + \underset{r}{\mathrm{Ind}}\, N)\,(mod\ \varphi(m))$$

البرهان : لدينا

$$MN = r^{\mathrm{Ind}\, MN}\ ,\ M = r^{\mathrm{Ind}\, M}\ ,\ N = r^{\mathrm{Ind}\, N} \Rightarrow M.N = r^{\mathrm{Ind}\, M + \mathrm{Ind}\, N}$$

ومنه

$$r^{\operatorname{Ind}_r MN} \equiv r^{\operatorname{Ind}_r M + \operatorname{Ind}_r N} \pmod m \Leftrightarrow \operatorname{Ind}_r MN \equiv \operatorname{Ind}_r M + \operatorname{Ind}_r N \pmod{\varphi(m)}$$

٣) $\operatorname{Ind}_r M^k \equiv k \operatorname{Ind}_r M \pmod{\varphi(m)} \qquad k>0$

البرهان : لدينا $M^k \equiv r^{\operatorname{Ind}_r M^k} \pmod m$

ومن جهة أخرى $M^k \equiv \left(r^{\operatorname{Ind}_r M}\right)^k \equiv r^{k \operatorname{Ind}_r M} \pmod m$

ومنه فإن $\operatorname{Ind}_r M^k \equiv k \operatorname{Ind}_r M \pmod{\varphi(m)}$

نتيجة لما سبق نلاحظ أن $\operatorname{Ind}_r 1 \equiv 0 \pmod{\varphi(m)}$

$\operatorname{Ind}_r r \equiv 1 \pmod{\varphi(m)}$

٤) إذا كان s, r جذرين أوليين مختلفين للعدد m فإن :

$$\operatorname{Ind}_r N \equiv (\operatorname{Ind}_s N)(\operatorname{Ind}_r s) \pmod{\varphi(m)}$$

البرهان : لدينا $N \equiv r^{\operatorname{Ind}_r N} = s^{\operatorname{Ind}_s N} \pmod m$

ولكن $s \equiv r^{\operatorname{Ind}_r s} \pmod m$

ومنه $N = r^{\operatorname{Ind}_r N} \equiv r^{(\operatorname{Ind}_r s)\operatorname{Ind}_s N} \pmod m$

الأمر الذي يكافىء :

$$\operatorname{Ind}_r N \equiv (\operatorname{Ind}_s N)(\operatorname{Ind}_r S) \bmod (\varphi(m))$$

- **نتيجة :** إذا كان $N=r$ نجد :

$$\operatorname{Ind}_r r \equiv 1 \equiv (\operatorname{Ind}_s r)(\operatorname{Ind}_r S) \equiv 1 \pmod{\varphi(m)}$$

تمرين : 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

٤-٤ حل التطابقات غير الخطية باستخدام الأدلة :

تستخدم الأدلة في إيجاد حلول بعض التطابقات غير الخطية وسنبين ذلك في الأمثلة التالية :

تمرين (١) : لنوجد حلول التطابق : $7x^3 \equiv 3 \pmod{13}$

الحل : رأينا أن العدد 2 هو جذر أولي للعدد 13 ، لنأخذ الدليل لطرفي التطابق بالنسبة للأساس 2 فنجد حسب خواص الأدلة :

حيث $\varphi(13) = 12$, $\operatorname{Ind}_2 7 + 3(\operatorname{Ind}_2 x) \equiv \operatorname{Ind}_2 3 \pmod{12}$

وباستخدام جدول الأدلة التالي للعدد 13 بالنسبة للأساس 2

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

نجد :

$$11 + 3(\operatorname{Ind}_2 x) \equiv 4 \pmod{12}$$

وبفرض $\operatorname{Ind}_2 x \equiv y$ نجد $3y \equiv 5 \pmod{12}$

ولما كان $(3,12) = 3$, $3 \nmid 5$ فليس للتطابق الخطي الأخير حل مما يدل على أنه ليس للتطابق الأصلي حل .

تمرين (٢) : لنوجد حلول التطابق : $7x^3 \equiv 4 \pmod{13}$

باستخدام الطريقة المستخدمة في التمرين (١) نجد أنه لحل التطابق يكفي إيجاد حلول التطابق الخطي : $3y \equiv 3 \pmod{12}$

لدينا هنا $(3,12) = 3$, $3|3$ 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

$$y = \operatorname{Ind}_{2} x$$

نجد أن حلول التطابق هي :

$$x \equiv 5 \ (mod\ 13) \ , \ x \equiv 6 \ (mod\ 13) \ , \ x \equiv 2 \ (mod\ 13)$$

تمارين

١- أوجد مراتب الأعداد 5 , 3 , 2 بالمقاسات التالية

أ - بالمقاس 17 ب - بالمقاس 19 جـ - بالمقاس 23

٢- 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

٣- أوجد مرتبة كل من العددين 19 , 11 بالمقاس 36 .

٤- أثبت أن 2 هو جذر أولي للعدد 19 وأنه ليس جذراً أولياً للعدد 17

٥- أثبت أنه لا يوجد للعدد 15 أي جذر أولي .

٦- أوجد جذرين أوليين للعدد 10 .

٧- أوجد جميع الجذور الأولية للعدد 17 علماً أن 3 هو جذر أولي له .

٨- أوجد حلول التطابقات

$$3x^3 \equiv 3 \pmod{13}, \quad x^8 \equiv 10 \pmod{13}, \quad 3x^6 \equiv 4 \pmod{13}$$

٩- اكتب جدول الأدلة للعدد 17 بالنسبة للجذر الأولي 3 ثم أوجد حلول التطابقات :

$$7x \equiv 7 \pmod{17}, \quad 9x^8 \equiv 8 \pmod{17}, \quad x^{12} \equiv 13 \pmod{17}$$

* * *

الملحق (١)

الأعداد المتحابة والعرب

لقد نشر الدكتور رشدي راشد الباحث في مركز البحوث التاريخية بباريس في فرنسا (فرنسي من أصل عربي) في مجلة تاريخ العلوم العربية (المجلد ٦) عام ١٩٨٢ التي تصدر عن معهد التراث العلمي العربي في جامعة حلب تحقيقاً لخمسة نصوص عربية تبين أهمية ما قدم العلماء العرب والمسلمون في نظرية الأعداد من إسهامات ومما ينسب لعلماء غربيين مثل فيرما وباسكال وديكارت وغيرهم وهذه النصوص هي :

- النص الأول لـ **كمال الدين الفارسي** في " الأعداد المتحابة "
- النص الثاني لـ **التنوخي**
- النص الثالث لـ **محمد باقر زين العابدين اليزدي**
- النص الرابع لـ **ابن البناء المراكشي** : " رفع الحجاب عن وجوه أعمال الحساب " .
- النص الخامس لـ **ابن هيرو التادلي**.

ونقدم فيما يأتي للقارئ مقدمة بحث الدكتور راشد حيث يقول :

ستبين النصوص التي ننشرها ههنا محققة مدى ما بلغته نظرية الأعداد الأولية من تقدم ومدى ما وصل إليه حساب التوافقات من نتائج على أيدي من كتب بالعربية في أواخر القرن الثالث عشر الميلادي خاصة .

فالنص الأول ، وهو أهمها بكثير ، يكفي وحده لبيان خطأ من توهم – وهم أكثر المؤرخين – أن نظرية الأعداد هي أفقر فروع الرياضيات العربية قاطبة . وكيف يكون هذا الوهم ممكناً ؟ أليس من العجيب ألا تتطور نظرية الأعداد بعد

ما حققه الجبر الحسابي من تقدم بفضل الكرخي ومدرسته ؟ وكذلك ستطيح هذه النصوص بوهم آخر ، ألا وهو خطأ من ظن أن اللجوء إلى المثلث الحسابي لدراسة مجموعات الأعداد المثلثة وما فوقها من المراتب وأن التفسير التوافقي لعناصر المثلث الحسابي ، هما من مكتسبات القرن السابع عشر.

فبعد قراءة هذه النصوص سنرى ، بما لا يدع مجالاً للشك ، أن نظرية الأعداد لم تقف عند تراث الإسكندرية، أي عند نقل وشرح الكتب العددية من " أصول " أقليدس " ومقدمة " نيقوماخوس ، بل لا نقف حتى عند مازاده ثابت بن قرة – وخاصة نظريته في الأعداد المتحابة – وغيره من أمثال عبد القاهر البغدادي. فنظرية الأعداد ذهبت إلى أبعد من ذلك بكثير بفضل الجبر، أو على وجه التحديد بفضل تطبيق الوسائل الجبرية التي ابتدعها الكرخي ومدرسته في دراسة الأعداد وخصائصها . ولعل أهم نتيجة لهذا التطبيق هو ظهور فصل جديد في نظرية الأعداد لم يكن معروفاً من قبل ، لا بهذا الاتساع ولا بهذه الصورة التي نجده عليها في الرياضيات العربية ، فضلاً عن أسلوب حديث في النظر والبرهان ، سيكون هو أسلوب نظرية الأعداد فيما بعد حتى سنة ١٦٤٠ على الأقل .أما هذا الفصل الجديد ، فيتضمن كل ما لا غنى عنه في البحث عن خصائص أجزاء الأعداد وقواسمها ، وهذه الخصائص نفسها . والباعث وراء هذه الدراسات لم يكن إلا البحث عن برهان آخر غير برهان ثابت بن قره للبرهان على نظريته عن الأعداد المتحابة . وأما الأسلوب الحديث فهو توافقي ، جبري ، فلم يعد هندسياً دون أن يصبح عددياً خالصاً .

هذه هي بالجملة مميزات النص الأساسي الذي نقدمه ههنا ، وهو رسالة كمال الدين الفارسي في الأعداد المتحابة ، التي تضم بين قضاياها كثيراً مما ينسب عادة إلى علماء القرنين السادس عشر والسابع عشر ، أو ما بعدهما أحياناً .

ونجد بين هذه القضايا :

- أول صياغة معروفة حتى يومنا هذا لما يُسمى بنظرية الحساب الأساسية ، أي أن كل عدد يمكن تحليله وبصورة واحدة إلى عناصر أولية منتهية العدة .
- أول دراسة معروفة لبعض خصائص تابع عدد أجزاء العدد وتابع عدد قواسمه؛ ومن ثم أول دراسة معروفة للتوابع الحسابية الأولية، التي كانت تُعزى ،هي وكثير من القضايا التي برهن عليها الفارسي، إلى ديكارت وآخرين من بعده .

ومما ينبغي التنبه له هو لجوء الفارسي إلى المثلث الحسابي لدراسة مجموعات الأعداد المثلثة وما فوقها من المراتب . واضطره هذا إلى تفسير توافقي لا غموض فيه لهذا المثلث ، وهو التفسير الذي كان ينقص الكرخي والسموءل من بعده كما بينا في مقاله أخرى ، والذي سيقوم به باسكال مرة أخرى . ومن الملاحظ أن الفارسي لا يقف عند هذا التطبيق وعند تلك العبارات التوافقية للتفسير والشرح ؛ مما يدل على أنها كانت شائعة مألوفة في عصره .

وينهي الفارسي رسالته هذه بحساب ما سُمي بعددي فيرما ، أي ١٧٢٩٦ و ١٨٤١٦، وبالبرهان على أنهما متحابان .

ونستطيع الآن أن نقطع بأن رياضيي هذا العصر كانوا على معرفة بهذين العددين ، ولكن لا يمكننا أن نقرر من هو أول العارفين بهذا الأمر . فنحن لا ندري بالدقة متى كان تحرير الفارسي لكتابه ، إلا أن هذا قد تم قبل عام ١٣٢٠ م وهو تاريخ وفاة الفارسي . ولكن النص الثاني الذي ننشره هنا ، وهو نص التنوخي ، الذي حرره سنة ١٣٠٧ م يضم العددين والبرهان على تحابهما . فكل ما نستطيع أن نقوله الآن هو أنه بين ١٣٠٧م–١٣٢٠ م

على أكثر تقدير كان هناك على الأقل شاهدان على ما أثبتنا . بل يمكننا أن نزيد على هذا ونبين(بفضل النص الثالث) أن العددين المتحابين – ٩٣٦٣٥٨٤ و ٩٤٣٧٠٥٦ – اللذين يحملان اسم ديكارت كان قد تم حسابهما على يدي محمد باقر بن زين العابدين اليزدي قبل الفيلسوف بقليل .

أما النص الرابع فهو لابن البناء المراكشي ، وهو فصل من كتاب المُسمى بـ " رفع الحجاب عن وجوه أعمال الحساب" . وهذا الكتاب هو تفسير وشرح لكتابه المعروف " تلخيص أعمال الحساب كتبه ١٣٠١– ١٣٠٢ م" أو كما قال هو نفسه وشرح مقصده في مقدمة "رفع الحجاب" : ((فإن كتابي الذي وضعته في تلخيص أعمال الحساب ، وتقريب معانيه ، وضبط قواعده ومعانيه ، وقد جمع صناعة العدد العملية بصنفي المعلوم والمجهول . فأردت إيضاح ما يغُمَّنه من العلم ، وشرح ما يظن غير المُحصل أنه مستغلق فيه على الفهم ، وبيان أصول القواعد والمباني)) .

وإذ قد أتينا بهذا النص هنا (أي المجلد ٦ ..) فلما يحتويه من قضايا رياضية في حساب التوافقات ، وايضاً للدلالة التاريخية التّي يدل عليها .

أما النص الخامس فهو لبيان مدى انتشار عددي فيرما بين الرياضين والشراح فهذا النص يبين لنا أن مؤلفه المتوفى في أوائل القرن الخامس عشر الميلادي وهو ابن هيرو التادلي من شراح ابن البناء المراكشي كان على معرفة بهذين العددين كما كان يريد أن يحرر رسالة يأتي فيها بالبرهان على تحاب الأعداد .

الملحق (٢)

ابن الهيثم ومبرهنة ويلسون

ثمة مخطوطة لابن الهيثم في نظرية الأعداد عنوانها :

" قول للحسن بن الحسن بن الهيثم في استخراج مسألة عددية "

قد حققها وعلق عليها الباحث في مركز البحوث التاريخية بباريس في فرنسا العلامة د . رشدي راشد (فرنسي من أصل عربي مصري) وفيه قد بين بالحجة الواضحة أن ابن الهيثم قد سبق عالم الرياضيات ويلسون في النص على خاصة مميزة للأعداد الأولية والتي يمكن أن تصاغ على النحو الآتي :

يكون العدد الطبيعي p أولياً (أي لا يقبل القسمة إلا على نفسه وعلى الواحد) إذا وفقط إذا كان العدد الآتي : $n = 2 \times 3 \times ..... \times (p-1) + 1$

يقبل القسمة على p (دون باق) وبلغة ابن الهيثم :

((إن كل عدد أول – وهو الذي لا يعده إلا الواحد فقط – فإنه إذا ضربت الأعداد التي قبله بعضها في بعض وزيد على ما يجتمع واحد كان الذي يجتمع إذا قسم على كل واحد من الأعداد التي قبل العدد الأول بقي منه واحد وإذا قسم على العدد الأول لم يبق منه شيء))

وقد بدأ ابن الهيثم طرح مسألته بأسلوب تعليمي تربوي فقدم لها سبق بمثال قائلاً :

((نريد أن نجد عدداً إذا قسم على اثنين بقي منه واحد ، وإن قسم على ثلاثة بقي منه واحد و إن قسم على أربعة بقي منه واحد وإن قسم على خمسة بقي منه واحد وإن قسم على ستة بقي منه واحد وإن قسم على سبعة لم يبق منه شيء))

ثم يقول هذه مسألة سيّالة أعني لها أجوبة كثيرة ، ولوجودهـا طريقـان أحـد الطريقيين وهو القانون < وهو الأسهل > : أن نضرب الأعداد المذكورة بعضها في بعض فما اجتمع زيد عليه واحد وهو العدد المطلوب.

وعليه وفقاً لهذا سيكون العدد : $6!+1=(2\times3\times4\times5\times6)+1=n_0$ (الحل القانوني) الذي يساوي 721 وهو العدد المطلوب الذي على الصفة المتقدم ذكرها ثم يقدم الطريقة الأخرى التي تبين أن لهذه المسألة حلولاً أخرى بل عدة أجوبـة بل أجوبة بلا نهاية (على حد تعبيره)

أول هذه الأجوبة 301 ثانيها 721 وهكذا :

$$301\ ,\ 721\ ,\ 1141\ ,\ 1511\ ,\ 1981\ ,\ ..$$

ونرى أنها متوالية حسابية حدها الأول 301 وأساسها 420 وكل حد من حدودها هو حل للمسألة المذكورة وسنترك لك قراءة المخطوطة في الصفحات الآتية .

بسم الله الرحمن الرحيم

العزة لله(*)

قول للحسن بن الحسن بن الهيثم في استخراج مسألة(١) عددية:

المسألة: نريد أن نجد عدداً إذا قسم على اثنين بقي منه واحد وإن قسم على ثلاثة بقي منه واحد وإن قسم على أربعة بقي منه واحد وإن قسم على خمسة بقي منه واحد وإن قسم على ستة بقي منه واحد وإن قسم على سبعة لم يبق منه شيء. الجواب: هذه المسألة سيالة، أعني لها أجوبة كثيرة، ولوجودها طريقان. أحد الطريقين وهو القانون أن نضرب الأعداد المذكورة التي يقسم عليها العدد بعضها في بعض فما اجتمع منها يزاد عليه واحد، وهو العدد المطلوب. أعني أن نضرب اثنين في ثلاثة ثم ما اجتمع منه في أربعة ثم ما اجتمع منه في خمسة ثم ما اجتمع منه في ستة ثم يزاد على ما اجتمع من ذلك واحد، وهو العدد المطلوب. والذي يجتمع من ضرب هذه الأعداد بعضها في بعض على الترتيب الذي ذكرناه هو ٧٢٠ ، فيزاد على ٧٢٠ واحد فيكون ٧٢١ فهو العدد. وذلك أن ٧٢٠ تنقسم(٢) على اثنين لأن لها نصف وتنقسم(٢) على ثلاثة لأن لها ثلث وتنقسم(٢) على أربعة لأن لها ربع وتنقسم(٢) على خمسة لأن لها خمس وتنقسم(٢) على ستة لأن لها سدس، وإذا كانت ٧٢٠ تنقسم(٢) على كل واحد من هذه الأعداد، فإن ٧٢١ (٣) إذا قسمت على كل واحد من هذه الأعداد بقي منها أبداً واحد، و٧٢١ تنقسم(٢) على ٧ لأن لها سبع. فالعدد المطلوب الذي على الصفة المتقدم ذكرها هو ٧٢١ . وقد يوجد العدد المطلوب بطريق آخر وهو الطريق الذي به نبين(٤) أن لهذه المسألة عدّة أجوبة، بل أجوبة بلا نهاية. وهو أن يوجد أقل عدد له نصف وثلث وربع وخمس وسدس، أعني أقل عدد يعدّه الأعداد التي قبل السبعة، وهو ستون. ونقسم(٥) الستين على سبعة فيبقى أربعة، فنطلب(٦) عدداً له سبع وإذا نقص منه واحد كان للباقي(٧) ربع. وقد يوجد أعداد كثيرة على هذه الصفة، وطريق وجود هذه الأعداد هو أن يؤخذ السبعة فينقص منها واحد فيبقى ستة فيضاف إلى ستة سبعة سبعة إلى أن ينتهي إلى عدد له ربع. فإذا انتهى التزيّد إلى عدد له ربع أضيف إلى ذلك العدد واحد فيكون للجميع سبع.

(*) قمنا بتنقيط النص في كثير من المواضع وأضفنا الهمزات وأثبتنا الأصل إذا اشتبه الأمر فقط، واستعملنا الرموز التالية في التحقيق: <. . . .> نقترح إضافة ما بينهما حتى يستقيم المعنى، [. . . .] نقترح حذف ما بينهما.

والنص هو مخطوطة «India office Library 80th-734,» (ff.121)

(١) مسئلة: وردت هكذا في النص ولن نشير إليها مرة أخرى.

(٢) ينقسم: وهي جائزة على اعتبار العدد ولكننا آثرنا التصحيح.

(٣) أعاد الناسخ ٧٢ تحت ٧٢ من ٧٢١.

(٤) تبين (٥) ويقسم (٦) فيطلب (٧) الباقي.

ومثال ذلك: يضاف إلى الستة سبعة فيكون ١٣ وليس لها ربع، فيضاف إلى ١٣ سبعة فيكون ٢٠ ولها ربع، فيضاف إلى ٢٠ واحد فيكون ٢١ ولها سبع، فيؤخذ ربع ٢٠ وهو ٥ فيضرب في ٦٠ فيكون ثلاثمائة فيضاف إليها واحد فيكون ٣٠١ وهو العدد المطلوب. وذلك أن ٣٠٠ لها نصف وثلث وربع وخمس وسدس، فالثلاثمائة تنقسم[7] على ٢ وعلى ٣ وعلى ٤ < وعلى ٥ > وعلى ٦ ، وإذا كانت ٣٠٠ تنقسم[7] على هذه الأعداد ولا يبقى منها شيء فالثلاثمائة[8] وواحد إذا قسمت على كل واحد من هذه الأعداد بقي منها واحد، و٣٠١ لها سبع فهي تنقسم[7] على ٧ ولا يبقى منها شيء، فالثلاثمائة والواحد هو العدد المطلوب. وأيضاً فإنا إذا أخذنا الستة وأضفنا إليها سبعة سبعة حتى يصير ٢٠ ثم أضفنا إليها بعد ذلك سبعة سبعة أربع مرات كان لما يجتمع ربع وكان إذا زيد عليه واحد كان لما يجتمع سبع. وإذا أضيف إلى ٢٠ سبعة سبعة أربع مرات كان من ذلك ٤٨ ولها ربع، وإذا أضيف إلى ٤٨ واحد كان ٤٩ ولها سبع، فيؤخذ ربع ٤٨ وهو ١٢ فيضرب في ٦٠ فيكون ٧٢٠ فيضاف إليها واحد فيكون ٧٢١ وهو العدد المطلوب، وهو العدد الذي خرج بالوجه الأول. وكذلك إن أضيف إلى ٤٨ سبعة سبعة أربع مرات صارت ٧٦ ولها ربع وإذا أضيف إلى ٧٦ واحد صارت ٧٧ ولها سبع، فيؤخذ ربع ٧٦ وهو ١٩ فيضرب في ٦٠ فيكون ١١٤٠ فيضاف إليه واحد فيكون ١١٤١ وهو العدد المطلوب. وذلك <أن> ١١٤٠ لها نصف وثلث وربع[8] وخمس/ وسدس، و١١٤١ لها سبع. وأيضاً فإنه إذا أضيف إلى ٧٦ سبعة سبعة أربع مرات كان من ذلك ١٠٤ ، فإذا أخذ ربعها وهو ٢٦ وضرب في ٦٠ وأضيف إلى ما يخرج من الضرب واحد كان ذلك هو العدد المطلوب. وكذلك دائماً كلما أضيف إلى العدد الذي ينتهي إليه سبعة سبعة أربع مرات وأخذ ربع ما اجتمع وضرب في ٦٠ وزيد عليه واحد كان منه العدد المطلوب.

فعلى هذا الوجه يمكن أن يوجد أعداد بلا نهاية كل واحد منها ينقسم على ٢ و٣ و٤ و٥ و٦ ويبقى من كل واحد منها واحد و<كل> واحد منها ينقسم على سبعة. وإذا كان ذلك فإنه بدل[9] ما يزاد على ٢٠ سبعة سبعة أربع مرات ويؤخذ ربع ما يجتمع يزاد على ٥ التي هي ربع ٢٠ سبعة واحدة فيكون ١٢ . وكذلك ٤٨ بدل[9] ما يزاد عليها سبعة سبعة أربع مرات ويؤخذ ربع ما يجتمع يزاد على ١٢ سبعة واحدة. وطريق وجود الأعداد المطلوبة هو أن يؤخذ ربع ٢٠ وهو ٥ ويزاد عليها سبعة سبعة أبداً بلا نهاية، ثم كل واحد من هذه الأعداد إذا ضرب في ٦٠ وزيد على ما اجتمع واحد كان كل واحد من الأعداد التي تجتمع[10] على هذا الترتيب هو العدد المطلوب. وهذا هو الجواب عن المسألة.

---

(٨) كتب الراء فوق السطر ثم أعاد «ربع» تحت الكلمة.

(٩) يدل (١٠) يجتمع

وإذ قد تبيّن ذلك فإنا نقول إن هـذا المعنى يلزم في كل عدد أول، أعني أن كل عـدد أول ـ وهو الذي لا يعدّه إلاّ الواحد فقط ـ فإنه إذا ضربت الأعداد التي قبله بعضها في بعض على الوجـه الذي قدمنا وزيد على ما يجتمع واحد كان الذي يجتمع إذا قسم على كل واحـد من الأعداد التي قبـل العدد الأول بقي منه واحد وإذا قسم على العدد الأول لم يبق منه شيء.

وعلى الوجه الآخر أيضاً: إذا وجد أقـل عدد يعـدّه الأعداد التي قبـل العدد الأول، أعني أقـل عدد له الأجزاء السمّية الأعداد التي قبل العدد الأول، ثم قسم هذا العـدد على العـدد الأول فما بقي حُفظ، ونحفظ الجزء السمّي لهذه البقية لنجعل القياس إليه. كما[11] إذا قسم عدد ٦٠ على ٧ منه ٤ والجزء[12] السمّي لها ـ الـذي هو الـربع ـ كـان القياس. والجـزء السمّي للعدد هـو الذي يعـدّ العدد الذي هو جزء له مرات بقدر آحـاد العدد الـذي يقال لـه إنه سمّيـه. فإذا حفظ الجـزء الـسمّي للبقية يؤخذ العدد الأول فينقص منه واحد كما فعل بالسبعة فما بقي يضاف إليـه العدد مـرة بعد مـرة إلى أن ينتهي إلى عدد له الجزء السمّي للبقية، أعني الجزء الذي حفظ، ثم يؤخذ من هذا العدد الذي ينتهي إليه الجزء السمّي للبقية ويضرب في العدد الذي هو أقـل عدد لـه الأجزاء السمّيـة الأعداد التي قبـل العدد الأول، فما خرج يضاف إليه واحد، وهـو العدد المطلوب. ثم إذا أضيـف إلى العدد الـذي هو الجزء السمّي للبقية العدد الأول مرة بعد مرة ثم ضرب[13] كل واحد من هذه الأعداد في العـدد الذي هو أقل عدد له الأجزاء[14] المذكورة واحداً[15] بعد واحد وزيد على كـل واحد [كـل واحد] منهـا واحد كان كل واحد من الأعداد التي تجتمع على هذه الصفة هـو العدد المطلوب. كما إذا ضرب كـل واحد من ١٢ و١٩ في ٦٠ [16] وزيـد على <كـل> واحد مما يخرج من الضرب واحـد كـان منـه العـدد المطلوب. فإن قسم <عدد من الأعداد التي تجتمع على هذه الصفة على> العدد الذي هو أقـل عدد له الأجزاء السمّية الأعداد التي قبل العدد الأول [و] كان الذي يبقى واحـد فقط، [<ثم> نقص من العدد الأول واحد وضرب الباقي <بعد أن قسم على الذي هو أقل عدد له الأجـزاء السمّية الأعـداد التي قبل العدد الأول وأضيف إلى ما اجتمع سبعة مرة بعـد مرة كم شئنـا> في العدد الـذي هو أقـل عدد له الأجزاء السمّية الأعداد التي قبل العدد الأول، فما خرج يزاد عليه واحد وهو العدد المطلوب.

فإذا سلكت هذه الطريقة في كل عدد أول كان كل عدد يوجد على هذا الوجه إذا قسم على كل واحد من الأعداد التي قبل العدد الأول بقي منـه واحد وإذا قسم عـلى العدد الأول لم يبق منـه شيء. فهذا الذي ذكرناه بستوعب[17] أحوبة جميع المسائل التي من هذا الجنس وبالله التوفيق.

تم جواب المسألة العددية والحمد لله رب العـالمين والصلوة عـلى رسولـه محمد المصـطفى وآله أجمعين.

---

(١١) كيما
(١٢) وبالجز
(١٣) صرف
(١٤) الأحر
(١٥) واحد، وفوقها علامة قد تكون الألف الذي نسيها الناسخ ثم عاد فأضافها.
(١٦) كتبها أولاً ٢٠ ثم صححها عليها ثم أعاد الستة تحتها.
(١٧) بسوخب.

الملحق (٣)

جدول الأعداد الأولية p حيث $2 \le p \le 5003$ وأصغر جذورها الأولية r :

$$\left(r^{p-1} = 1 \bmod p\right)$$

Table of Primes

(r denotes the least positive primitive root of the prime p)

p	r	p	r	p	r	p	r
2	1	89	3	199	3	337	10
3	2	97	5	211	2	347	2
5	2	101	2	223	3	394	2
7	3	103	5	227	2	353	3
11	2	107	2	229	6	359	7
13	2	109	6	233	3	367	6
17	3	113	3	239	7	373	2
19	2	127	3	241	7	379	2
23	5	131	2	251	6	383	5
29	2	137	3	257	3	389	2
31	3	139	2	263	5	397	5
37	2	149	2	269	2	401	3
41	6	151	6	271	6	409	21
43	3	157	5	277	5	419	2
47	5	163	2	281	3	421	2
53	2	167	5	283	3	431	7
61	2	173	2	293	2	433	5
67	2	179	2	307	5	439	15
71	7	181	2	311	17	443	2
73	5	191	19	313	10	449	3
79	3	193	5	317	2	457	13
83	2	197	2	331	3	461	2

(تابع) جدول الأعداد الأولية p حيث $2 \le p \le 5003$ وأصغر جذورها الأولية r

p	r	p	r	p	r	p	r
463	3	613	2	757	2	881	3
467	2	617	3	761	6	883	2
479	13	619	2	769	11	887	5
487	3	631	3	773	2	907	2
491	2	641	3	787	2	911	17
499	7	643	11	797	2	919	7
503	5	647	5	809	3	929	3
509	2	653	2	811	3	937	5
521	3	659	2	821	2	941	2
523	2	661	2	823	3	947	2
541	2	673	5	827	2	953	3
547	2	677	2	811	3	967	5
557	2	683	5	821	2	971	6
563	2	691	3	823	3	977	3
569	3	701	2	827	2	983	5
571	3	709	2	829	2	991	6
577	5	719	11	839	11	997	7
587	2	727	5	853	2	1009	11
593	3	733	6	857	3	1013	3
599	7	739	3	859	2	1019	2
601	7	743	5	863	5	1021	10
607	3	751	3	877	2	1031	14

(تابع) جدول الأعداد الأولية p حيث $2 \le p \le 5003$ وأصغر جذورها الأولية r

p	r	p	r	p	r	p	r
1033	5	1193	3	1361	3	1511	11
1039	3	1201	11	1367	5	1523	2
1049	3	1213	2	1373	2	1531	2
1051	7	1217	3	1381	2	1543	5
1061	2	1213	5	1399	13	1549	2
1063	3	1229	2	1909	3	1553	3
1069	6	1231	3	1423	3	1559	19
1087	3	1237	2	1427	2	1567	3
1091	2	1249	7	1429	6	1571	2
1093	5	1259	2	1433	3	1579	3
1097	3	1277	2	1439	7	1583	5
1103	5	1279	3	1447	3	1597	11
1109	2	1283	2	1451	2	1601	3
1117	2	1289	6	1453	2	1607	5
1123	2	1291	2	1459	3	1609	7
1129	11	1297	10	1471	6	1613	3
1151	17	1301	2	1481	3	1619	2
1153	5	1303	6	1483	2	1621	2
1163	5	1307	2	1487	5	1627	3
1171	2	1319	13	1489	14	1637	2
1181	7	1321	13	1493	2	1657	11
1187	2	1327	3	1499	2	1663	3

(تابع) جدول الأعداد الأولية p حيث $2 \le p \le 5003$ وأصغر جذورها الأولية r

p	r	p	r	p	r	p	r
1667	2	1879	6	2063	5	2273	3
1669	2	1889	3	2069	2	2281	7
1693	2	1901	2	2081	3	2287	19
1697	3	1907	2	2083	2	2293	2
1699	3	1913	3	2087	5	2297	5
1709	3	1931	2	2131	2	2309	2
1721	3	1933	5	2131	10	2311	3
1723	3	1949	2	2141	2	2333	2
1733	2	1951	3	2143	3	2339	2
1741	2	1973	2	2153	3	2341	7
1747	2	1979	2	2161	23	2347	3
1753	7	1987	2	2179	7	2351	13
1759	6	1993	5	2203	5	2357	2
1777	5	1997	2	2207	5	2371	2
1823	5	1999	3	2213	2	2377	5
1831	3	2003	5	2221	2	2381	3
1847	5	2011	3	2237	2	2383	5
1861	2	2017	5	2239	3	2389	2
1867	2	2027	2	2243	2	2437	2
1871	14	2029	2	2251	7	2441	6
1873	10	2039	7	2267	2	2447	5
1877	2	2053	2	2269	2	2459	2

(تابع) جدول الأعداد الأولية p حيث $2 \le p \le 5003$ وأصغر جذورها الأولية r

p	r	p	r	p	r	p	r
2467	2	2671	7	2851	2	3083	2
2473	5	2677	2	2857	11	3089	3
2477	2	2683	2	2861	2	3109	6
2503	3	2687	5	2879	7	3119	7
2521	17	2689	19	2887	5	3121	7
2531	2	2693	2	2897	3	3137	3
2539	2	2699	2	2903	5	3163	3
2543	5	2707	2	2909	2	3167	5
2549	2	2711	7	2917	5	3169	7
2551	6	2749	6	2927	5	3181	7
2557	2	2753	3	2939	2	3187	2
2579	2	2767	3	2953	13	3191	11
2591	7	2777	3	2957	2	3203	2
2593	7	2789	2	2963	2	3209	3
2609	3	2791	6	2969	3	3217	5
2617	5	2797	2	2971	10	3221	10
2621	2	2801	3	2999	17	3229	6
2633	3	2803	2	3001	14	3251	6
2647	3	2819	2	3011	2	3253	2
2657	3	2833	5	3019	2	3257	3
2659	2	2837	2	3023	5	3259	3
2663	5	2843	2	3037	2	3271	3

(تابع) جدول الأعداد الأولية p حيث $2 \le p \le 5003$ وأصغر جذورها الأولية r

p	r	p	r	p	r	p	r
3299	2	3517	2	3673	5	3911	13
3301	6	3527	5	3677	2	3917	2
3307	2	3529	17	3691	2	3919	3
3313	10	3533	2	3733	2	3923	2
3319	6	3539	2	3739	7	3929	3
3323	2	3541	7	3761	3	3931	2
3329	3	3547	2	3767	5	3943	3
3331	3	3557	2	3769	7	3947	2
3343	5	3559	3	3793	2	3967	6
3347	2	3571	2	3797	5	3989	2
3359	11	3581	2	3803	2	4001	3
3361	22	3583	3	3821	3	4003	2
3371	2	3593	3	3823	3	4007	5
3433	5	3607	5	3833	3	4013	2
3449	3	3613	2	3847	5	4019	2
3457	7	3617	3	3851	2	4073	3
3461	2	3623	5	3553	2	4079	11
3463	3	3631	15	3863	5	4091	2
3467	2	3637	2	3877	2	4093	2
3469	2	3643	2	3881	13	4099	2
3499	2	3659	2	3889	11	4111	12
3511	7	3671	13	3907	2	4127	5

(تابع) جدول الأعداد الأولية p حيث $2 \le p \le 5003$ وأصغر جذورها الأولية r

p	r	p	r	p	r	p	r
4129	13	4327	3	4561	11	4793	3
4133	2	4337	3	4567	3	4799	7
4139	2	4339	10	4583	5	4801	7
4153	5	4349	2	4591	11	4813	2
4157	2	4357	2	4597	5	4817	3
4177	3	4421	3	4603	2	4831	3
4201	5	4423	3	4621	2	4861	11
4211	11	4441	21	4637	2	4871	11
4217	6	4447	3	4639	3	4877	2
4219	3	4451	2	4643	5	4889	3
4229	2	4457	3	4649	3	4903	3
4231	2	4481	3	4663	3	4933	2
4241	3	4483	2	4673	3	4937	3
4243	2	4493	2	4679	11	4943	7
4253	2	4507	2	4691	2	4951	6
4259	2	4513	7	4703	5	4967	2
4261	2	4517	2	4759	3	4969	5
4271	7	4519	3	4783	6	4973	11
4273	5	4523	5	4787	2	4987	2
4283	2	4547	2	4789	2	4993	5
4289	3	4549	6	4909	6	4999	3
4297	5	4651	3	4919	13	5003	2
4463	5	4657	15	4931	6		

الملحق (٤)

جدول أعداد ميرسن الأولية:

المكتشفة حتى عام 2005 وعددها 42 ولها الشكل $n = 2^p - 1$

#	p	عدد الأرقام	سنة	ا سم المكتشف
1	2	1	antiquity	
2	3	1	antiquity	
3	5	2	antiquity	
4	7	3	antiquity	
5	13	4	1461	Reguis (1536), Cataldi (1603)
6	17	6	1588	Cataldi (1603)
7	19	6	1588	Cataldi (1603)
8	31	10	1750	Euler (1772)
9	61	19	1883	Pervouchine (1883), Seelhoff (1886)
10	89	27	1911	Powers (1911)
11	107	33	1913	Powers (1914)
12	127	39	1876	Lucas (1876)
13	521	157	Jan. 30, 1952	Robinson
14	607	183	Jan. 30, 1952	Robinson
15	1279	386	Jan. 30, 1952	Robinson
16	2203	664	Jan. 30, 1952	Robinson
17	2281	687	Jan. 30, 1952	Robinson

(تابع) جدول أعداد ميرسن الأولية				
#	p	عدد الأرقام	سنة	اسم المكتشف
18	3217	969	Sep. 8, 1957	Riesel
19	4253	1281	Nov. 3, 1961	Hurwitz
20	4423	1332	Nov. 3, 1961	Hurwitz
21	9689	2917	May 11, 1963	Gillies (1964)
22	9941	2993	May 16, 1963	Gillies (1964)
23	11213	3376	Jun. 2, 1963	Gillies (1964)
24	19937	6002	Mar. 4, 1971	Tuckerman (1971)
25	21701	6533	Oct. 30, 1978	Noll and Nickel (1980)
26	23209	6987	Feb. 9, 1979	Noll (Noll and Nickel 1980)
27	44497	13395	Apr. 8, 1979	Nelson and Slowinski (Slowinski 1978-79)
28	86243	25962	Sep. 25, 1982	Slowinski
29	110503	33265	Jan. 28, 1988	Colquitt and Welsh (1991)
30	132049	39751	Sep. 20, 1983	Slowinski
31	216091	65050	Sep. 6, 1985	Slowinski

(تابع) جدول أعداد ميرسن الأولية				
#	p	عدد الأرقام	سنة	ا سم المكتشف
32	756839	227832	Feb. 19, 1992	Slowinski and Gage
33	859433	258716	Jan. 10, 1994	Slowinski and Gage
34	1257787	378632	Sep. 3, 1996	Slowinski and Gage
35	1398269	420921	Nov. 12, 1996	Joel Armengaud/GIMPS
36	2976221	895832	Aug. 24, 1997	Gordon Spence/GIMPS (Devlin 1997)
37	3021377	909526	Jan. 27, 1998	Roland Clarkson/GIMPS
38	6972593	2098960	Jun. 1, 1999	Nayan Hajratwala/GIMPS
39	13466917	4053946	Nov. 14, 2001	Michael Cameron/GIMPS (Whitehouse 2001, Weisstein 2001)
40?	20996011	6320430	Nov. 17, 2003	Michael Shafer/GIMPS (Weisstein 2003)
41?	24036583	7235733	May 15, 2004	Josh Findley/GIMPS (Weisstein 2004)
42?	25964951	7816230	Feb. 18, 2005	Martin Nowak/GIMPS (Weisstein 2005)

للإستزادة والإطلاع : يمكنك العودة إلى الموقع

http://mathhworld.wolfram.com/ MersennePrime.html

الملحق (٥)

جدول قيم بعض الدوال الحسابية

ϕ,τ,σ

n	ϕ	τ	σ
1	1	1	1
2	1	2	3
3	2	2	4
4	2	3	7
5	4	2	6
6	2	4	12
7	6	2	8
8	4	4	15
9	6	3	13
10	4	4	18
11	10	2	12
12	4	6	28
13	12	2	14
14	6	4	24
15	8	4	24
16	8	5	31
17	16	2	18
18	6	6	39
19	18	2	20
20	8	6	42
21	12	4	32
22	10	4	36
23	22	2	24
24	8	8	60

(تابع) جدول قيم بعض الدوال الحسابية

n	ϕ	τ	σ
25	20	3	31
26	12	4	42
27	18	4	40
28	12	6	56
29	28	2	30
30	8	8	72
31	30	2	32
32	16	6	63
33	20	4	48
34	16	4	54
35	24	4	48
36	12	9	91
37	36	2	38
38	18	4	60
39	24	4	56
40	16	8	90
41	40	2	42
42	12	8	96
43	42	2	44
44	20	6	84
45	24	6	84
46	22	4	72
47	46	2	48
48	16	10	124
49	42	3	57

(تابع) جدول قيم بعض الدوال الحسابية

n	ϕ	τ	σ
50	20	6	93
51	32	4	72
52	24	6	98
53	52	2	54
54	18	8	120
55	40	4	72
56	24	8	120
57	36	4	80
58	28	4	90
59	58	2	60
60	16	12	168
61	60	2	62
62	30	4	96
63	36	6	104
64	32	7	127
65	48	4	84
66	20	8	144
67	66	2	68
68	32	6	126
69	44	4	96
70	24	8	144
71	70	2	72
72	24	12	195
73	72	2	74
74	36	4	114

الملحق (٦)

جدول أصغر قاسم أولي

يعطينا هذا الجدول أصغر قاسم أولي لكل عدد مؤلف أقل من 2047

ماعدا التي تقبل القسمة على أي من الأعداد الأولية 2,3,5,11

169	13	713	13	1037	17	1387	19	1751	17
221	13	731	17	1073	29	1391	13	1763	41
247	13	767	13	1079	13	1403	23	1769	29
289	17	799	19	1081	23	1411	17	1781	13
299	13	793	13	1121	19	1417	13	1807	13
323	17	799	17	1139	17	1457	31	1817	23
361	19	817	19	1147	31	1469	13	1819	17
377	13	841	29	1157	13	1501	19	1929	31
391	17	851	23	1159	19	1513	17	1843	19
403	13	871	13	1189	29	1517	37	1849	43
437	19	893	19	1207	17	1537	29	1853	17
481	13	899	29	1219	23	1541	23	1891	31
493	17	901	17	1241	17	1577	19	1909	23
527	17	923	13	1247	29	1591	37	1919	19
529	23	943	23	1261	13	1633	23	1921	17
533	13	949	13	1271	31	1643	31	1927	41
551	19	961	31	1273	19	1649	17	1937	13
559	13	989	23	1313	13	1651	13	1943	29
589	19	1003	17	1333	31	1679	23	1957	19
611	13	1007	19	1339	13	1681	41	1961	37
629	17	1027	13	1343	17	1691	19	1963	13
667	23	1037	17	1349	19	1703	13	2021	43
689	13	1073	17	1357	23	1711	29	2033	19
697	17	1007	19	1363	29	1717	17	2041	13
703	19	1027	13	1369	37	1739	37	2047	23

الملحق (٧)

جدول مربعات الأعداد من 1 حتى 1000

n	n^2	n	n^2	n	n^2	n	n^2
1	1	28	784	55	3025	82	6724
2	4	29	841	56	3136	83	6889
3	9	30	900	57	3249	84	7056
4	16	31	961	58	3364	85	7225
5	25	32	1024	59	3481	86	7396
6	36	33	1089	60	3600	87	7569
7	49	34	1156	61	3721	88	7744
8	64	35	1225	62	3844	89	7921
9	81	36	1296	63	3969	90	8100
10	100	37	1369	64	4096	91	8281
11	121	38	1444	65	4225	92	8464
12	144	39	1521	66	4356	93	8649
13	169	40	1600	67	4489	94	8836
14	196	41	1681	68	4624	95	9025
15	225	42	1764	69	4761	96	9216
16	256	43	1849	70	4900	97	9409
17	289	44	1936	71	5041	98	9604
18	324	45	2025	72	5184	99	9801
19	361	46	2116	73	5329	100	10000
20	400	47	2209	74	5476	101	10201
21	441	48	2304	75	5625	102	10404
22	484	49	2401	76	5776	103	10609
23	529	50	2500	77	5929	104	10816
24	576	51	2601	78	6084	105	11025
25	625	52	2704	79	6241	106	11236
26	676	53	2809	80	6400	107	11449
27	729	54	2916	81	6561	108	11664

n	n^2	n	n^2	n	n^2	n	n^2
109	11881	140	19600	171	29241	202	40804
110	12100	141	19881	172	29584	203	41209
111	12321	142	20164	173	29929	204	41616
112	12544	143	20449	174	30276	205	42025
113	12769	144	20736	175	30625	206	42436
114	12996	145	21025	176	30976	207	42849
115	13225	146	21316	177	31329	208	43264
116	13456	147	21609	178	31684	209	43681
117	13689	148	21904	179	32041	210	44100
118	13924	149	22201	180	32400	211	44521
119	14161	150	22500	181	32761	212	44944
120	14400	151	22801	182	33124	213	45369
121	14641	152	23104	183	33489	214	45796
122	14884	153	23409	184	33856	215	46225
123	15129	154	23716	185	34225	216	46656
124	15376	155	24025	186	34596	217	47089
125	15625	156	24336	187	34969	218	47524
126	15876	157	24649	188	35344	219	47961
127	16129	158	24964	189	35721	220	48400
128	16384	159	25281	190	36100	221	48841
129	16641	160	25600	191	36481	222	49284
130	16900	161	25921	192	36864	223	49729
131	17161	162	26244	193	37249	224	50176
132	17424	163	26569	194	37636	225	50625
133	17689	164	26896	195	38025	226	51076
134	17956	165	27225	196	38416	227	51529
135	18225	166	27556	197	38809	228	51984
136	18496	167	27889	198	39204	229	52441
137	18769	168	28224	199	39601	230	52900
138	19044	169	28561	200	40000	231	53361
139	19321	170	28900	201	40401	232	53824

n	n^2	n	n^2	n	n^2	n	n^2
233	54289	264	69696	295	87025	326	106276
234	54756	265	70225	296	87616	327	106929
235	55225	266	70756	297	88209	328	107584
236	55696	267	71289	298	88804	329	108241
237	56169	268	71824	299	89401	330	108900
238	56644	269	72361	300	90000	331	109561
239	57121	270	72900	301	90601	332	110224
240	57600	271	73441	302	91204	333	110889
241	58081	272	73984	303	91809	334	111556
242	58564	273	74529	304	92416	335	112225
243	59049	274	75076	305	93025	336	112896
244	59536	275	75625	306	93636	337	113569
245	60025	276	76176	307	94249	338	114244
246	60516	277	76729	308	94864	339	114921
247	61009	278	77284	309	95481	340	115600
248	61504	279	77841	310	96100	341	116281
249	62001	280	78400	311	96721	342	116964
250	62500	281	78961	312	97344	343	117649
251	63001	282	79524	313	97969	344	118336
252	63504	283	80089	314	98596	345	119025
253	64009	284	80656	315	99225	346	119716
254	64516	285	81225	316	99856	347	120409
255	65025	286	81796	317	100489	348	121104
256	65536	287	82369	318	101124	349	121801
257	66049	288	82944	319	101761	350	122500
258	66564	289	83521	320	102400	351	123201
259	67081	290	84100	321	103041	352	123904
260	67600	291	84681	322	103684	353	124609
261	68121	292	85264	323	104329	354	125316
262	68644	293	85849	324	104976	355	126025
263	69169	294	86436	325	105625	356	126736

n	n^2	n	n^2	n	n^2	n	n^2
357	127449	388	150544	419	175561	450	202500
358	128164	389	151321	420	176400	451	203401
359	128881	390	152100	421	177241	452	204304
360	129600	391	152881	422	178084	453	205209
361	130321	392	153664	423	178929	454	206116
362	131044	393	154449	424	179776	455	207025
363	131769	394	155236	425	180625	456	207936
364	132496	395	156025	426	181476	457	208849
365	133225	396	156816	427	182329	458	209764
366	133956	397	157609	428	183184	459	210681
367	134689	398	158404	429	184041	460	211600
368	135424	399	159201	430	184900	461	212521
369	136161	400	160000	431	185761	462	213444
370	136900	401	160801	432	186624	463	214369
371	137641	402	161604	433	187489	464	215296
372	138384	403	162409	434	188356	465	216225
373	139129	404	163216	435	189225	466	217156
374	139876	405	164025	436	190096	467	218089
375	140625	406	164836	437	190969	468	219024
376	141376	407	165649	438	191844	469	219961
377	142129	408	166464	439	192721	470	220900
378	142884	409	167281	440	193600	471	221841
379	143641	410	168100	441	194481	472	222784
380	144400	411	168921	442	195364	473	223729
381	145161	412	169744	443	196249	474	224676
382	145924	413	170569	444	197136	475	225625
383	146689	414	171396	445	198025	476	226576
384	147456	415	172225	446	198916	477	227529
385	148225	416	173056	447	199809	478	228484
386	148996	417	173889	448	200704	479	229441
387	149769	418	174724	449	201601	480	230400

n	n^2	n	n^2	n	n^2	n	n^2
481	231361	512	262144	543	294849	574	329476
482	232324	513	263169	544	295936	575	330625
483	233289	514	264196	545	297025	576	331776
484	234256	515	265225	546	298116	577	332929
485	235225	516	266256	547	299209	578	334084
486	236196	517	267289	548	300304	579	335241
487	237169	518	268324	549	301401	580	336400
488	238144	519	269361	550	302500	581	337561
489	239121	520	270400	551	303601	582	338724
490	240100	521	271441	552	304704	583	339889
491	241081	522	272484	553	305809	584	341056
492	242064	523	273529	554	306916	585	342225
493	243049	524	274576	555	308025	586	343396
494	244036	525	275625	556	309136	587	344569
495	245025	526	276676	557	310249	588	345744
496	246016	527	277729	558	311364	589	346921
497	247009	528	278784	559	312481	590	348100
498	248004	529	279841	560	313600	591	349281
499	249001	530	280900	561	314721	592	350464
500	250000	531	281961	562	315844	593	351649
501	251001	532	283024	563	316969	594	352836
502	252004	533	284089	564	318096	595	354025
503	253009	534	285156	565	319225	596	355216
504	254016	535	286225	566	320356	597	356409
505	255025	536	287296	567	321489	598	357604
506	256036	537	288369	568	322624	599	358801
507	257049	538	289444	569	323761	600	360000
508	258064	539	290521	570	324900	601	361201
509	259081	540	291600	571	326041	602	362404
510	260100	541	292681	572	327184	603	363609
511	261121	542	293764	573	328329	604	364816

n	n^2	n	n^2	n	n^2	n	n^2
605	366025	636	404496	667	444889	698	487204
606	367236	637	405769	668	446224	699	488601
607	368449	638	407044	669	447561	700	490000
608	369664	639	408321	670	448900	701	491401
609	370881	640	409600	671	450241	702	492804
610	372100	641	410881	672	451584	703	494209
611	373321	642	412164	673	452929	704	495616
612	374544	643	413449	674	454276	705	497025
613	375769	644	414736	675	455625	706	498436
614	376996	645	416025	676	456976	707	499849
615	378225	646	417316	677	458329	708	501264
616	379456	647	418609	678	459684	709	502681
617	380689	648	419904	679	461041	710	504100
618	381924	649	421201	680	462400	711	505521
619	383161	650	422500	681	463761	712	506944
620	384400	651	423801	682	465124	713	508369
621	385641	652	425104	683	466489	714	509796
622	386884	653	426409	684	467856	715	511225
623	388129	654	427716	685	469225	716	512656
624	389376	655	429025	686	470596	717	514089
625	390625	656	430336	687	471969	718	515524
626	391876	657	431649	688	473344	719	516961
627	393129	658	432964	689	474721	720	518400
628	394384	659	434281	690	476100	721	519841
629	395641	660	435600	691	477481	722	521284
630	396900	661	436921	692	478864	723	522729
631	398161	662	438244	693	480249	724	524176
632	399424	663	439569	694	481636	725	525625
633	400689	664	440896	695	483025	726	527076
634	401956	665	442225	696	484416	727	528529
635	403225	666	443556	697	485809	728	529984

n	n^2	n	n^2	n	n^2	n	n^2
729	531441	754	568516	779	606841	804	646416
730	532900	755	570025	780	608400	805	648025
731	534361	756	571536	781	609961	806	649636
732	535824	757	573049	782	611524	807	651249
733	537289	758	574564	783	613089	808	652864
734	538756	759	576081	784	614656	809	654481
735	540225	760	577600	785	616225	810	656100
736	541696	761	579121	786	617796	811	657721
737	543169	762	580644	787	619369	812	659344
738	544644	763	582169	788	620944	813	660969
739	546121	764	583696	789	622521	814	662596
740	547600	765	585225	790	624100	815	664225
741	549081	766	586756	791	625681	816	665856
742	550564	767	588289	792	627264	817	667489
743	552049	768	589824	793	628849	818	669124
744	553536	769	591361	794	630436	819	670761
745	555025	770	592900	795	632025	820	672400
746	556516	771	594441	796	633616	821	674041
747	558009	772	595984	797	635209	822	675684
748	559504	773	597529	798	636804	823	677329
749	561001	774	599076	799	638401	824	678976
750	562500	775	600625	800	640000	825	680625
751	564001	776	602176	801	641601	826	682276
752	565504	777	603729	802	643204	827	683929
753	567009	778	605284	803	644809	828	685584

n	n^2	n	n^2	n	n^2	n	n^2
829	687241	854	729316	879	772641	904	817216
830	688900	855	731025	880	774400	905	819025
831	690561	856	732736	881	776161	906	820836
832	692224	857	734449	882	777924	907	822649
833	693889	858	736164	883	779689	908	824464
834	695556	859	737881	884	781456	909	826281
835	697225	860	739600	885	783225	910	828100
836	698896	861	741321	886	784996	911	829921
837	700569	862	743044	887	786769	912	831744
838	702244	863	744769	888	788544	913	833569
839	703921	864	746496	889	790321	914	835396
840	705600	865	748225	890	792100	915	837225
841	707281	866	749956	891	793881	916	839056
842	708964	867	751689	892	795664	917	840889
843	710649	868	753424	893	797449	918	842724
844	712336	869	755161	894	799236	919	844561
845	714025	870	756900	895	801025	920	846400
846	715716	871	758641	896	802816	921	848241
847	717409	872	760384	897	804609	922	850084
848	719104	873	762129	898	806404	923	851929
849	720801	874	763876	899	808201	924	853776
850	722500	875	765625	900	810000	925	855625
851	724201	876	767376	901	811801	926	857476
852	725904	877	769129	902	813604	927	859329
853	727609	878	770884	903	815409	928	861184

n	n^2	n	n^2	n	n^2		
929	863041	954	910116	979	958441		
930	864900	955	912025	980	960400		
931	866761	956	913936	981	962361		
932	868624	957	915849	982	964324		
933	870489	958	917764	983	966289		
934	872356	959	919681	984	968256		
935	874225	960	921600	985	970225		
936	876096	961	923521	986	972196		
937	877969	962	925444	987	974169		
938	879844	963	927369	988	976144		
939	881721	964	929296	989	978121		
940	883600	965	931225	990	980100		
941	885481	966	933156	991	982081		
942	887364	967	935089	992	984064		
943	889249	968	937024	993	986049		
944	891136	969	938961	994	988036		
945	893025	970	940900	995	990025		
946	894916	971	942841	996	992016		
947	896809	972	944784	997	994009		
948	898704	973	946729	998	996004		
949	900601	974	948676	999	998001		
950	902500	975	950625	1000	1000000		
951	904401	976	952576				
952	906304	977	954529				
953	908209	978	956484				

الملحق (٨)

بعض تطبيقات ماثماتيكا : Mathematica 5.0 في نظرية الأعداد

للإستزادة يمكنك العودة إلى الموقع :

http://www.columbia.edu/~rama /notbook.html

مرشحة ايراتوستين
Sieve of Eratosthenes

فيما يلي برنامج مكتوب باستخدام الماثماتيكا يمكن من إيجاد الأعداد الأولية التي لا تتجاوز عدداً حقيقياً موجباً معطى n باستخدام مرشحة ايراتوستين

```
In[3]:= SieveOfEratosthenes[n_]:=
          Module[ {t,P,i=1,x},
          t=N[Sqrt[n]];
          P=Range[2,n];
          While[ P[[i]] <= t,
               x=Table[k P[[i]],
                        {k,P[[i]], Floor[n/P[[i]]]}];
               P=Complement[P,x];
               i++
               ];
          Return[P]]
          SieveOfEratosthenes[100]

Out[4]= {2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41,
         43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89, 97}
```

لاحظ النتيجة التي حصلنا عليها من تطبيق البرنامج من أجل n=100 .

ثمة تعليمات باستخدامها نحصل على العدد الأولي ذي الترتيب المرغوب به

Untitled-1 *

```
In[8]:= primes[[10]]

Out[8]= 29
```

تعطي هذه التعليمة العدد الأولي ذي الترتيب العاشر

List of primes.nb

```
ListofPrimes[n_] := Prime[Range[n]]
ListofPrimes[100]

{2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47,
 53, 59, 61, 67, 71, 73, 79, 83, 89, 97, 101, 103, 107,
 109, 113, 127, 131, 137, 139, 149, 151, 157, 163, 167,
 173, 179, 181, 191, 193, 197, 199, 211, 223, 227, 229,
 233, 239, 241, 251, 257, 263, 269, 271, 277, 281,
 283, 293, 307, 311, 313, 317, 331, 337, 347, 349,
 353, 359, 367, 373, 379, 383, 389, 397, 401, 409,
 419, 421, 431, 433, 439, 443, 449, 457, 461, 463,
 467, 479, 487, 491, 499, 503, 509, 521, 523, 541}
```

برنامج إيجاد قائمة مرتبة من الأعداد الأولية طولها عدد معطى n.

قائمة بأول مئة عدد أولي (قائمة طولها 100)
طبق البرنامج من أجل 100000

خوارزمية اقليدس
Euclidean Algorithm

فيما يلي برنامج باستخدام الماثماتيكا يمكن من إيجاد مجموعة البواقي المتتالية التي تحصل من تطبيق خوارزمية اقليدس على العددين a , b

Euclidean Algorithm.nb *

```
In[38]:=
    EuclideanAlgorithmList[a_, b_] :=
     First /@
      Most[FixedPointList[{Last[#], Remainder @@#} &,
        {a, b}]]
    EuclideanAlgorithmList[42, 30]

Out[39]= {42, 30, 12, 6, 0}
```

مجموعة البواقي المتتالية * نتيجة لتطبيق خوارزمية اقليدس على العددين
42 , 30

برنامج إيجاد القاسم المشترك الأعظم لعددين صحيحين
a , b باستخدام خوارزمية اقليدس .

Euclidean Algorithm.nb

```
In[30]:= EuclideanAlgorithmGCD[a_, b_] :=
          FixedPointList[{Last[#], Remainder @@#} &,
            {a, b}][[-3, 1]]
         EuclideanAlgorithmGCD[42, 30]

Out[31]= 6
```

قارن مابين النتيجة التي حصلت عليها
هنا وما بين الباقي ما قبل الأخير في
مجموعة البواقي المتتالية *

الكسور المستمرة
Continued Fractions

برنامج إيجاد الكسر المستمر المنتهي الموافق $\langle a_1,\dots,a_n\rangle$ للكسر $\frac{A}{B}$

Continued Fractions.nb

```
In[3]:= Cfraction[A_, B_] :=
          If[Mod[A, B] == 0, Quotient[A, B],
           Flatten[{Quotient[A, B], Cfraction[B, Mod[A, B]]}]]
        Cfraction[257, 97]

Out[4]= {2, 1, 1, 1, 5, 1, 4}
```

النتيجة التي حصلنا عليها من أجل A=257 و B=97

$$\frac{257}{97}=\langle 2,1,1,1,5,1,4\rangle$$

برنامج إيجاد الكسر $\frac{A}{B}$ الموافق للكسر المستمر المنتهي $\langle a_1,\ldots,a_n \rangle$

Continued Fractions.nb

```
In[5]:= fraction[a_List] :=
        If[Length[a] == 1, First[a],
         First[a] + 1/fraction[Rest[a]]]
        fraction[{2, 1, 1, 1, 5, 1, 4}]
```

Out[8]= $\frac{257}{97}$

النتيجة التي حصلنا عليها من أجل الكسر المنتهي $\langle 2,1,1,1,5,1,4 \rangle$

أي:

$$\langle 2,1,1,1,5,1,4 \rangle = \frac{257}{97}$$

برنامج إيجاد الكسور المتتالية الموافقة للكسور الجزئية المستمرة المنتهية من الكسر المستمر المنتهي الموافق لـــ $\frac{A}{B}$

Continued Fractions.nb *

```
In[7]:= convergents[frac_List] :=
        Module[{p, q, n, c}, n = Length[frac];
         p[-1] = 1;
         p[0] = frac[[1]];
         q[-1] = 0;
         q[0] = 1;
         Do[p[i] = frac[[i + 1]] p[i - 1] + p[i - 2], {i, 1, n - 1}];
         Do[q[i] = frac[[i + 1]] q[i - 1] + q[i - 2], {i, 1, n - 1}];
         c = Table[p[i] / q[i], {i, 0, n - 1}];
         Return[c]]
       convergents[Cfraction[257, 97]]
```

$$\text{Out[8]=}\ \left\{2,\ 3,\ \frac{5}{2},\ \frac{8}{3},\ \frac{45}{17},\ \frac{53}{20},\ \frac{257}{97}\right\}$$

النتيجة التي حصلنا عليها من تطبيق البرنامج من أجل الكسر المنتهي المستمر الموافق للكسر $\frac{257}{97}$

لاحظ :

$$\langle 2\rangle = 2$$

$$\langle 2,1\rangle = 3$$

$$\langle 2,1,1\rangle = \frac{5}{2}$$

$$\langle 2,1,1,1\rangle = \frac{8}{3}$$

.....

وهكذا ....

نظرية الباقي الصينية
Chinese Remainder Theorem

برنامج إيجاد أصغر حل مشترك موجب
لمجموعة من التطابقات بالنسبة لمقاسات أولية
نسبياً مثنى باستخدام طريقة البواقي الصينية

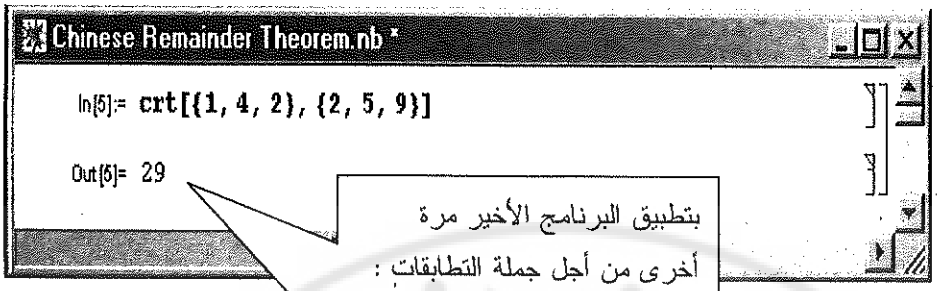
Chinese Remainder Theorem.nb *

```
crt[a_List, m_List]:= Module[ {i,x,n,k },
        i=1; x= a[[1]]; n=m[[1]];

      If[ Length[a]== Length[m],
       k=Length[a];
           While[ i<k,
                  i++;
                  {u,v}= ExtendedGCD[m[[i]], n][[2]];
                  x=u m[[i]] x + v n a[[i]] ;
                  n=m[[i]] n;
                  x=Mod[x,n]];
           Return[x],
       Return["Both lists have to be the same
 length"]]]
      crt[{1,2}, {2,3}]

Out[4]= 5
```

أصغر حلول جملة التطابقات :

$x \equiv 1 \bmod 2$

$x \equiv 2 \bmod 3$



بتطبيق البرنامج الأخير مرة أخرى من أجل جملة التطابقات :

$$x \equiv 1 \pmod 2$$

$$x \equiv 4 \pmod 5$$

$$x \equiv 2 \pmod 9$$

نحصل على أصغر الحلول الموجبة وهو : 29

ثبت المصطلحات (انكليزي- عربي)

A

Algorithm	خوارزمية
Euclidean_	خوارزمية اقليدس
Amicable pair	زوج متحاب

B

Base	أساس
Basic theorem	مبرهنة أساسية
Binomial	حداني
Bounds	حدود

C

Chinese remainder theorem	مبرهنة الباقي الصينية
Congruences	تطابقات
Linear___	تطابقات خطية
Conditional___	تطابقات شرطية
Identical___	تطابقات مطابقه
Equivalent___	تطابقات متكافئة
Quadratic___	تطابقات تربيعية

D

Digits	أرقام
Divisibility	قابلية القسمة
Divisor	قاسم

Common___	قاسم مشترك
Greatest Common___	قاسم مشترك أعظم
Diophantine Equations	معادلات ديوفانتس
Diophantus	ديوفانتس

E

Element	عنصر
Euler's method	طريقة اولر

F

Factorization	التحليل إلى عوامل
Fermat's Conjecture	حدس فيرما
Fermat's Little theorem	مبرهنة فيرما الصغرى
Fermat Last theorem	مبرهنة فيرما الكبرى
Finite Continued Fractions	الكسور المستمرة المنتهية
Function	دالة (تابع)
Euler's___	دالة اولر
The Greatest Integer___	دالة الجزء الصحيح
Liouville's ___	دالة لوفيل
Möbius___	دالة موبيوس
Multiplicative__	دالة ضربية
Number theoretic__	دالة عددية (حسابية)
Fundamental theorem of arithmetic	المبرهنة الأساسية في الحساب

I

Indices	الأدلة
Induction	استقراء
Mathematical Induction	استقراء رياضي
The Principle of mathematical____	مبدأ الاستقراء الرياضي
Integer	عدد صحيح
Least Common Multiple	مضاعف مشترك أصغر
Möbius Inversion formula	صيغة موبياس لتعاكس

N

Number	عدد
Composite ___	عدد مؤلف (مركب)
Fermat __	عدد فيرما
Mersenne__	عدد ميرسن
Perfect___	عدد كامل (تام)
Prime___	عدد أولي
The Prime Number Theorem	مبرهنة الأعداد الأولية
Primitive Root	جذر أولي (أو أصلي)
Pseudo Prime__	عدد شبه أولي
Pythagorean Triple	ثلاثي فيثاغورث
Primitive ___	ثلاثي فيثاغورث أولي (أصلي)

R

Residue	باقي
__Class	صف الباقي
Complete set of Residues	مجموعة بواقي تامة
Reduced set of Residues	مجموعة بواقي مختزلة
Quadratic Residue	باقي تربيعي
Sieve of Eratosthenes	غربال (مرشحة) ايراتوستين
Wilson	ويلسون

المراجع

1.
Adams, W.W. + Goldestein, L.
Introduction to Number Theory.
New Jersey . Englewood Cliffs 1976.

2.
Andrews ,G.
Number Theory ,
Hindustan Publishing Corporatwr (India) 1992

3.
Apostol, Tom.
Introduction to Analytic Number Theory ,
Springer International Student Edition Narosa Publishing House 1993.

4.
Archibald , R.
An Introduction to the Theory of Numbers ,
Charles E . Merrell Publishing Co . 1970

5.
Burton D.M.
Elementary Number Theory ,
Boston . Allyn Bacon Imc. Universal Book Stall 1994.

6.
Graham, R + Knuth, D + Patashnik, O.
Concrete Mathematics
Addisoun _ Wesley Publishing Company 1996

7.
Niver, I. and Zuckerman, H .
An Introduction to the Theory of Numbers ,
New York : John Wiley and Sons 1993.
8.
Ribernboim ,P
The Little Book of Big Primes ,
Springer – Verlag New York 1991

8.
Rose , H.E.
A Course in Number Theory ,
Oxford Science Publication 1996

9.
Rosen, K. H.
Elementary Number Theory and its Applications , 2 nd
New York Addison _ Wesle Publishing Co 1988

مراجع مساندة

1.
Child, L .
a Concrete introduction to high algebra
Springer ,1995.

2.
Crandall ,R + Pomerance,C :
Prime Numbers
Springer . 2005.

3.
Crandall, R , Pomerance ,c
Prime Numbers
Springer, 2005

4.
Jones G.A + Jones J . M ,
elementary number theory ,
Springer,1998

5.
Elliott,
Probabilistic Number Theory I
Springer,1979.

6.
Elliott,
Probabilistic Number Theory II,
Springer,1980.

7.
Kenneth, I +Rosen, M.
A classical Introduction to modern number Theory
2nd ed , Springer, 1990.

8.
Malik , S.B.
Basic Number Theory,
New Delhi : Vikas publishing Pvr Ltd 1995.

9.
NarKiewicz ,W
Elementary and Analytic Theory of Algebraic Numbers
Springer 3rd ed . 2004 .

10.
Penglley, D + Richman ,F.
Did Euclid Need the Euclidean Algorithm to Prove
Unique Factorization?
The American Mathematical Monthly.
volume 113, Number3, March, 2006.

١. رشدي راشد :
تاريخ الرياضيات العربية بين الجبر و الحساب .
مركز الدراسات الوحدة العربية ١٩٨٩_ بيروت .

٢. د. فوزي أحمد الذكير + د. معروف عبد الرحمن سمحان :
مقدمة في نظرية الأعداد ط٢ ٢٠٠٢م
دار النشر: دار الخريجي للنشر و التوزيع - السعودية .

٣. مجلة تاريخ العلوم الصادرة عن معهد التراث / المجلد ٦ / ١٩٨٠ .

٤. موسوعة الرياضيات العربية بإشراف د. رشدي راشد والصادرة عن مركز دراسات الوحدة العربية ١٩٩٧– بيروت.

المدققة اللغوية

د. عاطفة فيصل
قسم اللغة العربية وآدابها جامعة دمشق