Σ

p^2

p

الفصل الأول

$$x^2 + 2x = 3^n$$

تعريفات ونظريات أساسية

قسمة الأعداد الصحيحة (Division of Integers)

تعريف 1.

نقول إنَّ العدد الصحيح a، حيث $a \neq 0$، يقسم العدد الصحيح b، و نكتب $a|b$، إذا وُجِدَ عدد صحيح c يُحقِّق المساواة $b=ca$. في هذه الحالة نقول أيضاً إنَّ a عامل من عوامل b أو b قابل للقسمة على a أو b أحد مضاعفات a. إذا كان a لا يقسم b فإننا نكتب $a \nmid b$.

ملحوظة:

أ- من التعريف السابق، عند كتابة الرمز $a|b$ فإننا نفرض مُسبَقاً أن $a \neq 0$.

ب- عندما $a^k | b$ و $a^{k+1} \nmid b$ فإننا نكتب $a^k \| b$، أي أن k هو أكبر أُس للعدد a بحيث $a^k | b$. مثلاً نجد بسهولة أن $5^1 \| 70$ و $2^3 \| 40$ و $3^4 \| 324$.

نظرية 1.

لتكن a و b و c أعداداً صحيحة.

1. إذا كان $a \neq 0$ فإن $a|a$ و $a|0$.
2. لأي عدد صحيح a، $1|a$.
3. إذا كان $a|b$ فإن $a|bc$.
4. إذا كان $a|b$ و $b|c$ فإن $a|c$.
5. إذا كان $a|b$ و $a|c$ فإن $a|bx+cy$ لجميع الأعداد الصحيحة x و y.
6. إذا كان $a|b$ و $b|a$ فإن $a=\pm b$.

7. إذا كان $a|b$ و $a>0$ و $b>0$ فإن $a \le b$.

نظرية 2. (خوارزمية القسمة – *Division Algorithm*)

لأي عـددين صـحيحين a و b، حيـث $a>0$، يوجـد عـددان صحيحان وحيدان q و r يُحققان

$$b = qa + r$$

حيث $0 \le r < a$. العدد q يُسمى خارج قسمة b على a، و العدد r يُسمى باقي قسمة b على a.

ملحوظة: باستخدام خوارزمية القسمة يمكن تصنيف الأعداد الصحيحة بطرق مختلفة. على سبيل المثال، بالقسمة على 2، أي عدد صحيح يأخذ إحدى الصورتين الآتيتين $2q$ أو $2q+1$. وبالقسمة على 3، أي عدد صحيح يأخذ إحدى الصور الآتية $3q$ أو $3q+1$ أو $3q+2$.

مثال 1: أثبت أن $3|n(n+1)(n+2)$ لأي عدد صحيح n.

الحل: العدد n يأخذ إحدى الصور الآتية: $3q$ أو $3q+1$ أو $3q+2$.

- إذا كان $n=3q$ فإن $3|n$ ومن ثم $3|n(n+1)(n+2)$.
- إذا كـان $n=3q+1$ فـإن $n+2=3(q+1)$. هـذا يعنـي أن $3|n+2$ ومن ثم $3|n(n+1)(n+2)$.
- إذا كـان $n=3q+2$ فـإن $n+1=3(q+1)$. هـذا يعنـي أن $3|n+1$ ومن ثم $3|n(n+1)(n+2)$.

إذاً في جميع الحالات $3|n(n+1)(n+2)$.

مثال 2: أثبت أن $8|n^2-1$ لأي عدد صحيح فردي n.

الحل: بما أن n عدد فردي فإن $n=2k+1$ حيث k عدد صحيح. هذا

يقتضي أن

$$n^2-1=4k^2+4k=4k(k+1)$$

بما أن العددين k و $k+1$ عددان صحيحان متتاليان فلابد أن يكون أحدهما عدداً زوجياً. هذا يقتضي أن $2|k(k+1)$ ومن ثم $4\times 2|4k(k+1)$، أي أن $8|n^2-1$.

نظرية 3. (تمثيل الأعداد الصحيحة – *Representation of Integers*)

إذا كان a و b عددين صحيحين موجبين و $b>1$ فإنه يمكن كتابة a بطريقة و حيدة على الصورة

$$a=c_k b^k+c_{k-1}b^{k-1}+\cdots+c_1 b+c_0$$

حيث إنَّ $c_0,c_1,\cdots,c_k$ أعداد صحيحة تحقق $c_k\neq 0$ و $0\le c_i<b$ لجميع قيم $i=0,1,\cdots,k$. في هذه الحالة نقول إننا مثَّلنا أو كتبنا العدد a باستخدام الأساس b.

في حالة $b=10$ نحصل على التمثيل العشري للأعداد الصحيحة، أو تمثيل الأعداد الصحيحة باستخدام النظام العشري (Decimal System)، الذي يُكتَب بصورة مُختصرة كالآتي:

$$\begin{aligned}a&=c_k\times 10^k+c_{k-1}\times 10^{k-1}+\cdots+c_1\times 10+c_0\\&=c_k c_{k-1}\cdots c_1 c_0\end{aligned}$$

حيث $c_k\neq 0$ و $0\le c_i\le 9$ لجميع القيم $i=0,1,\ldots,k$. في هذه الحالة نقول إنَّ عدد الخانات العشرية للعدد a يُساوي $k+1$.

نتيجة 4.

عدد الخانات العشرية للعدد الصحيح الموجب N يساوي

$\llbracket \log_{10} N \rrbracket + 1$ حيث $\llbracket x \rrbracket$ يساوي أكبر عدد صحيح أقل من أو يساوي x.

مثال 3: عدد الخانات العشرية للعدد 7^{200} يساوي

$$\llbracket \log_{10} 7^{200} \rrbracket + 1 = \llbracket 200 \log_{10} 7 \rrbracket + 1 = \llbracket 169.02 \rrbracket + 1 = 170$$

تعريف 2. (القاسم المشترك الأكبر – *Greatest Common Divisor*)

نقول إنَّ العدد c قاسم مشترك للعددين a و b إذا كان $c | a$ و $c | b$.
إذا كان a و b ليس كلاهما صفراً، فأكبر قاسم مشترك للعددين a و b يُسمَّى **القاسم المشترك الأكبر** للعددين a و b، ويُرمَز له بالرمز (a,b).

ملحوظة: $(0,0)$ غير معرف. لذا عندما نكتب (a,b) فإننا نفترض مسبقاً أن أحد العددين a أو b لا يساوي صفراً.

نظرية 5.

$g = (a,b)$ إذا وفقط إذا تحققت الشروط التالية:

1. $g > 0$
2. $g | a$ و $g | b$.
3. إذا كان $c | a$ و $c | b$ فإن $c \le g$.

نظرية 6.

1. إذا كان $(a,b) = g$ فإنه يوجد عددان صحيحان x_0 و y_0 يحققان المساواة $g = ax_0 + by_0$.
2. إذا كان m عدد صحيح موجب فإن $(ma, mb) = m(a,b)$.
3. إذا كان $(a,b) = g$ فإن $(a/g, b/g) = 1$.

4. إذا كان $(a,c)=(b,c)=1$ فإن $(ab,c)=1$.
5. لأي عددٍ صحيح x يكون لدينا $(a,b)=(a,b+ax)$.
6. إذا كان $c\,|\,ab$ و $(c,b)=1$ فإن $c\,|\,a$.
7. إذا كان $a\,|\,c$ و $b\,|\,c$ و $(a,b)=1$ فإن $ab\,|\,c$.

تعريف 3.

إذا كان $(a,b)=1$ فإننا نقول إنَّ a و b **عددان أوليان نسبياً**. نقول إن الأعداد $a_1,a_2,\cdots,a_k$ **أعداد أولية نسبياً مثنى مثنى** إذا كان $(a_i,a_j)=1$ لكل $i \neq j$.

نظرية 7. (خوارزمية أُقليدس – *Euclidean Algorithm*)

ليكن a و b عددين صحيحين، حيث $a>0$. بتكرار خوارزمية القسمة، يصبح لدينا الآتي:

$$\begin{aligned}
b &= aq_1 + r_1, && 0<r_1<a\\
a &= r_1q_2 + r_2, && 0<r_2<r_1\\
r_1 &= r_2q_3 + r_3, && 0<r_3<r_2\\
&\vdots\\
r_{n-2} &= r_{n-1}q_n + r_n, && 0<r_n<r_{n-1}\\
r_{n-1} &= r_nq_{n+1}
\end{aligned}$$

عندئذ $(a,b)=r_n$ (آخر باقٍ لا يساوي الصفر في عملية القسمة)

يمكن إيجاد عددين صحيحين x و y يُحقِقان $(a,b)=ax+by$ عن طريق كتابة بواقي القسمة $r_1,r_2,\cdots,r_n$ كتراكيب خطية بدلالة a و b.

مثال 4: جِد قيمة $(312,27)$ ثم جِد عددين صحيحين x و y يُحقِقان

$(312,27)=312x+27y$.

الحل: باستخدام خوارزمية أقليدس نحصل على الآتي:

$$\begin{aligned}312&=27(11)+15\\27&=15(1)+12\\15&=12(1)+3\\12&=3(4)\end{aligned}$$

هذا يقتضي أن $(312,27)=3$. لإيجاد x و y نبدأ بالمساواة الثالثة:

$$\begin{aligned}3&=15-12(1)\\&=15-[27-15(1)](1)\\&=15(2)-27(1)\\&=[312-27(11)](2)-27(1)\\&=312(2)+27(-23)\end{aligned}$$

إذاً $x=2$ و $y=-23$.

مثال 5: ليكن $m>n$ عددين صحيحين موجبين. أثبت أنه إذا كان $(n+1,m+1)=1$ فإن $n+1\mid\binom{m}{n}$.

الحل: من العلاقة

$$\binom{m}{n}=\frac{m!}{n!\cdot(m-n)!}=\frac{n+1}{m+1}\cdot\frac{(m+1)!}{(n+1)!\cdot(m-n)!}$$
$$=\frac{n+1}{m+1}\cdot\binom{m+1}{n+1}$$

نستنتج أن

$$(m+1)\cdot\binom{m}{n}=(n+1)\cdot\binom{m+1}{n+1}$$

حيث إنَّ $n+1 \mid (m+1)\cdot\binom{m}{n}$ و $(n+1,m+1)=1$ فإن $n+1 \mid \binom{m}{n}$.

مثال 6: أثبت أن $(a^n-1,a^m-1)=a^{(n,m)}-1$ حيث $a>1, n\geq 1, m\geq 1$ أعداد صحيحة.

الحل: إذا كان $n=m$ فالنتيجة واضحة. لذا نفرض أن $n>m$ وأن $(n,m)=r_k$ حيث

$$\begin{aligned}
&n=mq_1+r_1, && 0<r_1<m\\
&m=r_1q_2+r_2, && 0<r_2<r_1\\
&\vdots\\
&r_{k-2}=r_{k-1}q_k+r_k, && 0<r_k<r_{k-1}\\
&r_{k-1}=r_kq_{k+1}.
\end{aligned}$$

من المعادلة الأولى نحصل على الآتي:

$$a^n-1=(a^m-1)(a^{n-m}+a^{n-2m}+a^{n-3m}+\cdots+a^{n-q_1m})+(a^{r_1}-1)$$

من ذلك نستنتج أن

$$(a^n-1,a^m-1)=(a^m-1,a^{r_1}-1)$$

بنفس الطريقة، المعادلات التالية سوف تُعطينا الآتي:

$$\begin{aligned}
&(a^m-1,a^{r_1}-1)=(a^{r_1}-1,a^{r_2}-1)\\
&\vdots\\
&(a^{r_{k-2}}-1,a^{r_{k-1}}-1)=(a^{r_{k-1}}-1,a^{r_k}-1)
\end{aligned}$$

الآن بما أن $r_{k-1}=r_kq_{k+1}$ فإن $a^{r_k}-1 \mid a^{r_{k-1}}-1$ ومن ثم

$$(a^{r_{k-1}}-1,a^{r_k}-1)=a^{r_k}-1=a^{(n,m)}-1$$

من المتساويات السابقة نحصل على المطلوب:

$$(a^n-1,a^m-1)=(a^m-1,a^{r_1}-1)=(a^{r_1}-1,a^{r_2}-1)$$
$$=\cdots=a^{(n,m)}-1$$

بنفس الطريقة نحصل على نفس النتيجة عند فرض $m>n$.

تعريف 4. (المضاعف المشترك الأصغر – *Least Common Multiple*)

نقول إنَّ العدد c مضاعف مشترك للعددين a و b إذا كان $a|c$ و $b|c$. إذا كان a و b عددين لا يساويان الصفر، فإن **المضاعف المشترك الأصغر** للعددين a و b، ونرمز لذلك بالرمز $[a,b]$، هو أصغر مضاعف مشترك موجب للعددين a و b.

نظرية 8.

$[a,b]=l$ إذا وفقط إذا تحققت الشروط التالية:

1. $l>0$
2. $a|l$ و $b|l$
3. إذا كان $a|c$ و $b|c$ فإن $c\geq l$.

نظرية 9.

ليكن $a\neq 0$ و $b\neq 0$ عددين صحيحين.

1. إذا كان $m>0$ فإن $[ma,mb]=m[a,b]$
2. $[a,b](a,b)=|ab|$
3. $(a,b)|[a,b]$

مثال 7: جِد جميع الأعداد الصحيحة الموجبة x و y التي تُحقِق $(x,y)=6$ و $[x,y]=60$.

الحل: حيث إنَّ $(x,y)=6$ فإنه يوجد عددان صحيحان موجبان a و b بحيث إنَّ $x=6a$ و $y=6b$ و $(a,b)=1$. من المعطى $[x,y]=60$ يصبح لدينا $60=[6a,6b]=6[a,b]=6ab$، أي أنَّ $ab=10$. هذا يعطينا

$$(a,b)=(1,10),(2,5),(5,2),(10,1)$$

و من ثم

$$(x,y)=(6,60),(12,30),(30,12),(60,6)$$

ملحوظة: القاسم المشترك الأكبر و المضاعف المشترك الأصغر لأكثر من عددين يُعَرَّف استقرائياً كما يلي:

$$(a_1,\cdots,a_{n-1},a_n)=((a_1,\cdots,a_{n-1}),a_n),$$
$$[a_1,\cdots,a_{n-1},a_n]=[[a_1,\cdots,a_{n-1}],a_n]$$

الأعداد الأولية (Prime Numbers)

تعريف 5.

نقول إنَّ العدد الصحيح p **عدد أولي** (Prime number) إذا كان $p>1$ وكانت قواسِمه الموجبة هي العدد نفسه p و العدد 1 فقط. إذا كان العدد a، حيث $a>1$، غير أولي فإننا نُسميه **عدداً مؤلَّفاً** (Composite number).

الأعداد الأولية الأُولى هي $2,3,5,7,11,13,17,19,23,29,\cdots$

نظرية 10.

ليكن p عدداً أولياً. إذا كان $p \mid ab$ فإن $p \mid a$ أو $p \mid b$.

نظرية 11. (النظرية الأساسية للحساب *Fundamental Theorem of Arithmetic-*)

أي عدد صحيح $n > 1$ يمكن كتابته بشكلٍ وحيد (باستثناء الترتيب) كحاصل ضرب عدد منتهٍ من الأعداد الأولية.

النظرية الأساسية للحساب تمكننا من كتابة أي عدد صحيح $n > 1$ على الصيغة

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_r^{\alpha_r}$$

حيث إنَّ p_i عدد أولي و $\alpha_i \geq 1$ لجميع قيم $i = 1, 2, \cdots, r$. نُطلِق على هذه الصيغة "**تحليل العدد n إلى عوامِلِهِ الأولية**".

نظرية 12. (نظرية أُقليدس)

يوجد عدد غير منتهٍ من الأعداد الأولية.

مثال 8: ليكن $a > 1$ و $b \neq 0$ عددين صحيحين. أثبت أنه إذا كان $a^2 \mid b^2$ فإن $a \mid b$.

الحل: توجد حالتان: إما $(a,3) = 1$ أو $(a,3) = 3$. إذا كان $(a,3) = 1$ فإن $a^2 \mid 3b^2$ يقتضي أنَّ $a^2 \mid 3b^2$ ومن ثم $a \mid b$. لنفرض الآن أنَّ $(a,3) = 3$. يمكن أن نكتب $a = 3^\alpha a_1$ و $b = 3^\beta b_1$، حيث $\alpha \geq 1$ و $\beta \geq 1$ و $(a_1, 3) = 1$ و $(b_1, 3) = 1$. إذا كان $a^2 \mid 3b^2$ فإن $3^{2\alpha} a_1^2 \mid 3^{2\beta+1} b_1^2$. هذا بدوره يقتضي أنَّ $a_1^2 \mid b_1^2$ و $2\alpha < 2\beta + 1$ و منه نستنتج أن $a_1 \mid b_1$ و

$\alpha \le \beta$، أي أنَّ $a|b$.

مثال 9: أثبت أن $\sqrt{p}$ عدد غير نسبي لأي عدد أولي p.

الحل: افترض أن $\sqrt{p}$ عدد نسبي، أي يوجد عددان صحيحان a و $b \neq 0$ بحيث

$$\sqrt{p} = \frac{a}{b}$$

نفرض أيضاً أنه لا يوجد أي عامل مشترك بين a و b، أي أن $(a,b)=1$. بتربيع الطرفين نحصل على $a^2 = pb^2$. هذا يقتضي أن $p|a^2$ ومن ثم $p|a$. بكتابة $a = pk$، حيث k عدد صحيح، وبالتعويض في المعادلة $a^2 = pb^2$ نحصل على المساواة $pk^2 = b^2$. منها نستنتج أن $p|b^2$ ومن ثم $p|b$. هذا يقتضي أن $(a,b) \neq 1$ وهذا يُناقِض ما افترضناه مُسبقاً من أن $(a,b)=1$. بسبب هذا التناقض نستنتج أن $\sqrt{p}$ عدد غير نسبي.

مثال 10: باستخدام المُتسلسلة $e = \sum_{k=0}^{\infty} \frac{1}{k!}$ أثبت أن العدد e عدد غير نسبي.

الحل: لتفرض أن e عدد نسبي ولنكتب $e = \frac{m}{n}$، حيث m و n عددان صحيحان موجبان. بضرب المُتسلسلة $e = \sum_{k=0}^{+\infty} \frac{1}{k!}$ في $n!$ نحصل على الآتي:

$$n!e = A_n + \frac{1}{n+1} + \frac{1}{(n+1)(n+2)} + \frac{1}{(n+1)(n+2)(n+3)} + \cdots$$

حيث $A_n = n!\left(1+\frac{1}{1!}+\frac{1}{2!}+\frac{1}{3!}+\cdots+\frac{1}{n!}\right)$ عدد صحيح. حيث إنَّ $n!e=(n-1)!m$ عدد صحيح فإن $n!e-A_n$ عدد صحيح أيضاً.
باستخدام خواص المتسلسلات الهندسية نستنتج الآتي:

$$0<n!e-A_n=\frac{1}{n+1}+\frac{1}{(n+1)(n+2)}+\frac{1}{(n+1)(n+2)(n+3)}+\cdots$$
$$<\frac{1}{n+1}+\frac{1}{(n+1)^2}+\frac{1}{(n+1)^3}+\cdots$$
$$=\frac{1/(n+1)}{1-[1/(n+1)]}=\frac{1}{n}<1$$

وهذا مستحيل لأنه لا يوجد عدد صحيح بين الصفر و الواحد. من ذلك نستنتج أنَّ e عدد غير نسبي.

متطابقات أساسية

ليكن a و b عددين حقيقيين.

1. نظرية ذات الحدَّين: إذا كان $n\geq 1$ عدداً صحيحاً فإن

$$(a+b)^n=\sum_{i=0}^{n}\binom{n}{i}a^i b^{n-i}$$

2. إذا كان $n\geq 1$ عدداً صحيحاً فإن

$$a^n-b^n=(a-b)(a^{n-1}+a^{n-2}b+\cdots+ab^{n-2}+b^{n-1})$$

3. إذا كان $n\geq 1$ عدداً صحيحاً فردياً فإن

$$a^n+b^n=(a+b)(a^{n-1}-a^{n-2}b+\cdots+ab^{n-2}-b^{n-1})$$

مثال 11: أثبت أنَّ $5\,|\,6^n+9$ لجميع الأعداد الصحيحة $n\geq 1$.

الحل: باستخدام نظرية ذات الحدين نحصل على

$$6^n+9=(5+1)^n+9=9+\sum_{i=0}^{n}\binom{n}{i}5^i=10+\sum_{i=1}^{n}\binom{n}{i}5^i$$

حيث إنَّ العدد 5 يقسم كل حد في الطرف الأيمن فإننا نستنتج من ذلك أنَّ $5\mid 6^n+9$.

مثال 12: اثبت أنَّ $13\mid 7^{21}+2^{21}$.

الحل: لاحظ أولاً أنَّ $7^{21}+2^{21}=(7^3)^7+(2^3)^7$. إذاً $7^3+2^3\mid 7^{21}+2^{21}$. بما أنَّ $7^3+2^3=351=3^3\times 13$ فإن $13\mid 7^{21}+2^{21}$.

المعادلات الديوفانتية الخطية (Linear Diophantine Equations)

نظرية 13.

ليكن c عدداً صحيحاً و a و b عددين صحيحين ليس كلاهما صفراً. ليكن $g=(a,b)$. إذاً توجد حلول صحيحة للمعادلة الخطية $ax+by=c$ إذا و فقط إذا كان $g\mid c$. إذا كان $x=x_0, y=y_0$ حلاً للمعادلة فإن جميع الحلول معطاة كالآتي:

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

حيث t عدد صحيح.

التطابقات (Congruences)

تعريف 6.

ليكن a و b و $m\geq 1$ أعداداً صحيحة. نقول إنَّ a **يطابق** b قياس m، ونرمز لذلك $a\equiv b \bmod m$، إذا كان $m\mid a-b$. في حالة $m\nmid a-b$ فإننا نقول إنَّ a **لا يطابق** b قياس m ونكتب

.$a \not\equiv b \mod m$

ملحوظة: من التعريف نلاحظ إنَّ $a \equiv b \mod m$ إذا و فقط إذا كان يوجد عدد صحيح k بحيث $a = b + km$.

نظرية 14. (خواص التطابقات)

ليكن a و b و c و d و $m \geq 1$ أعداداً صحيحة.

1. $a \equiv a \mod m$
2. إذا كان $a \equiv b \mod m$ فإن $b \equiv a \mod m$.
3. إذا كان $a \equiv b \mod m$ و $b \equiv c \mod m$ فإن $a \equiv c \mod m$.
4. إذا كان $a \equiv b \mod m$ و $c \equiv d \mod m$ فإن $a + c \equiv b + d \mod m$.
5. إذا كان $a \equiv b \mod m$ و $c \equiv d \mod m$ فإن $ac \equiv bd \mod m$.
6. إذا كان $a \equiv b \mod m$ فإن $a^k \equiv b^k \mod m$ لأي عدد صحيح موجب k.
7. إذا كان $a \equiv b \mod m$ و $d \mid m$، حيث $d > 0$، فإن $a \equiv b \mod d$.
8. إذا كان $a \equiv b \mod m$ و $c > 0$ فإن $ac \equiv bc \mod mc$.
9. $ax \equiv ay \mod m$ إذا و فقط إذا $x \equiv y \mod \dfrac{m}{(a,m)}$.
10. $x \equiv y \mod m_i$ ، حيث $i = 1, 2, \cdots, r$، إذا و فقط إذا $x \equiv y \mod [m_1, m_2, \cdots, m_r]$.

مثال 13: أثبت أنه إذا كان $c \mid a_i - 1$ لجميع القيم $1 \leq i \leq n$ فإن $c \mid a_1 a_2 \cdots a_n - 1$.

الحل: باستخدام التطابقات نلاحظ أنه إذا كان $c \mid a_i - 1$ فإن

$$a_i \equiv 1 \bmod c, \qquad 1 \le i \le n.$$

بضرب التطابقات السابقة ببعضها نحصل على التطابق

$$a_1 a_2 \cdots a_n \equiv 1 \bmod c$$

ومنه نحصل على المطلوب $c \mid a_1 a_2 \cdots a_n - 1$.

مثال 14: جِد باقي قسمة العدد $7^{123} + 11^{456}$ على 9.

الحل: حيث إن

$$7^{123} \equiv (-2)^{123} = -(2^3)^{41} \equiv -(-1)^{41} = 1 \bmod 9$$
$$11^{456} \equiv (2)^{456} = (2^3)^{152} \equiv (-1)^{152} = 1 \bmod 9$$

إذاً $7^{123} + 11^{456} \equiv 2 \bmod 9$. هذا يقتضي أن باقي قسمة العدد $7^{123} + 11^{456}$ على 9 يساوي 2.

مثال 15: أثبت أن $a^2 \equiv 0,\ 1,\ 4 \bmod 8$ لأي عدد صحيح a.

الحل: بكتابة $a = 4k + i$، حيث $i = 0, 1, 2, 3$، نجد أن $a^2 = 16k^2 + 8ki + i^2$ ومن ثم $a^2 \equiv i^2 \bmod 8$. بما أنَّ $i^2 \equiv 0,\ 1,\ 4 \bmod 8$، إذاً $a^2 \equiv 0,\ 1,\ 4 \bmod 8$.

مثال 16: جِد اختباراً لقابلية قسمة عددٍ صحيح على 8.

الحل: ليكن $n = a_m a_{m-1} \cdots a_3 a_2 a_1 a_0$ هو تمثيل العدد n باستخدام الأساس 10. أي أن

$$n = a_m \times 10^m + a_{m-1} \times 10^{m-1} + \cdots + a_3 \times 10^3 + a_2 \times 10^2 + a_1 \times 10 + a_0$$

بما أن $8 \mid 10^i$ لجميع القيم $i \ge 3$ فإننا نحصل على التطابق

$$n \equiv a_2 \times 10^2 + a_1 \times 10 + a_0 \equiv a_2 a_1 a_0 \mod 1000$$

هذا يقتضي أن $8|n$ إذا و فقط إذا كان $8|a_2a_1a_0$، أي أن العدد n يقبل القسمة على 8 إذا وفقط إذا كان العدد 8 يقسم العدد المُكوَّن من الأرقام الموجودة في منازل الآحاد والعشرات والمئات.

تعريف 7. (أنظمة الرواسب التامة و المختزلة- *Complete and Reduced Residue Systems*)

1. إذا كان $x \equiv a \mod m$ فإننا نقول إنَّ a **راسب** (Residue) للعدد x قياس m.

2. نقول عن مجموعة مكونة من m من الأعداد $c_1, c_2, \cdots, c_m$ إنها **نظام رواسب تام قياس** m إذا كان أي عدد صحيح يطابق قياس m عدداً واحداً فقط من الأعداد $c_1, c_2, \cdots, c_m$.

3. نقول عن مجموعة مكونة من الأعداد $r_1, r_2, \cdots, r_t$ إنها **نظام رواسب مختزَل قياس** m إذا كان أي عدد صحيح a، حيث $(a,m)=1$، يطابق قياس m عدداً واحداً فقط من الأعداد $r_1, r_2, \cdots, r_t$.

مثال 17:

أ- المجموعة $\{0,1,2,\cdots,m-1\}$ تُمثل نظام رواسب تام قياس m.

ب- إذا كان $m>0$ عدداً فردياً فإن المجموعة $\{0,\pm1,\pm2,\cdots,\pm\frac{m-1}{2}\}$ تُمثل نظام رواسب تام قياس m، وإذا كان $m>0$ عدداً زوجياً فإن المجموعة $\{0,\pm1,\pm2,\cdots,\pm\frac{m-2}{2},\pm\frac{m}{2}\}$ تُمثل نظام رواسب تام قياس m.

ت- إذا كان p عدداً أولياً فإن المجموعة $\{1,2,\cdots,p-1\}$ تُمثل نظام رواسب مختزَل قياس p .

نظرية 15.

جميع أنظمة الرواسب المختزَلة قياس m تحتوي على العدد نفسه من العناصر. نرمز لهذا العدد بـ $\phi(m)$. الدالة ϕ تُسمَّى **دالة أويلر.**

حيث إن المجموعة $\{0,1,2,\cdots,m-1\}$ تُمثل نظام رواسب تام قياس m، فإن المجموعة الجزئية من هذه المجموعة والمكونة من الأعداد الأولية نسبياً مع m تُكوِّن نظام رواسب مختزَل قياس m. بما أن عدد عناصر هذا النظام هو $\phi(m)$، فإنه بإمكاننا أن نُعرِّف دالة أويلر ϕ كما يلي:

تعريف 8.

ليكن m عدداً صحيحاً موجباً. $\phi(m)$ هو عدد الأعداد الموجبة الأولية نسبياً مع m والتي هي أقل من أو يساوي m.

نظرية 16.

1. إذا كان n و m عددين صحيحين موجبين بحيث إنَّ $(m,n)=1$، فإن $\phi(mn)=\phi(m)\phi(n)$.
2. إذا كان n عدداً صحيحاً موجباً و p عدداً أولياً فإن $\phi(p^n)=p^n-p^{n-1}=p^{n-1}(p-1)$.
3. إذا كان n عدداً صحيحاً موجباً فإن $\phi(n)=n\prod_{p|n}\left(1-\frac{1}{p}\right)$.

نظرية 17.

ليكن $(a,m)=1$. إذا كان $r_1,r_2,\cdots,r_n$ نظام رواسب تام (أو مختزَل) قياس m فإن $ar_1,ar_2,\cdots,ar_n$ نظام رواسب تام (أو مختزَل) قياس m.

نظرية 18.(نظرية فيرما – *Fermat's Theorem*)

ليكن p عدداً أولياً. إذا كان $(a,p)=1$ فإن $a^{p-1}\equiv 1 \bmod p$.

نتيجة 19.

إذا كان p عدداً أولياً فإن $a^p\equiv a \bmod p$ لأي عدد صحيح a.

نظرية 20.(نظرية أويلر - *Euler's Theorem*)

إذا كان $(a,m)=1$ فإن $a^{\phi(m)}\equiv 1 \bmod m$.

تعريف 9.

ليكن a و m عددين صحيحين حيث $m>1$. نقول إنَّ العدد الصحيح b هو معكوس ضربي قياس m للعدد a إذا كان $ab\equiv 1 \bmod m$. ◆

نظرية 21.

يوجد معكوس ضربي قياس m للعدد a إذا وفقط إذا كان $(a,m)=1$. في هذه الحالة، المعكوس الضربي هو معكوس وحيد قياس m: إذا كان x_1 و x_2 معكوسين ضربيين قياس m للعدد a فإن $x_1\equiv x_2 \bmod m$.

مثال 18: ليكن p عدداً أولياً. أثبت أن المعكوس الضربي قياس p للعدد

a، حيث $1 \le a \le p-1$، هو نفسه العدد a إذا وفقط إذا كان $a=1$ أو $a=p-1$.

الحل: إذا كان المعكوس الضربي قياس p للعدد a هو نفسه فإن $a^2 \equiv 1 \bmod p$. هذا يعني أنَّ $p \mid a^2-1=(a-1)(a+1)$ ومن ثم إما $p \mid a-1$ أو $p \mid a+1$، أي $a \equiv 1 \bmod p$ أو $a \equiv -1 \equiv p-1 \bmod p$ بما أنَّ $1 \le a \le p-1$، إذاً $a=1$ أو $a=p-1$. الإتجاه الآخر للإثبات واضح.

نظرية 22.(نظرية ويلسون -*Wilson's Theorem*)

إذا كان p عدداً أولياً فإن $(p-1)! \equiv -1 \bmod p$.

ملحوظة: عكس نظرية ويلسون أيضاً صحيح: إذا كان $n>1$ و $(n-1)! \equiv -1 \bmod n$ فإن n عدد أولي.

مثال 19: أثبت أن العدد n عدد أولي إذا وفقط إذا كان $\phi(n)=n-1$.

الحل: إذا كان n عدداً أولياً فمن الواضح أن $\phi(n)=n-1$. إذا كان n عدداً مؤلفاً فإن $n=ab$ حيث $1<a \le b<n$. هذا يقتضي أن $(n,a) \ne 1$. نستنتج من ذلك أن $\phi(n) \le n-2$ ومن ثم $\phi(n) \ne n-1$.

مثال 20: أثبت أنه إذا كان $d \mid n$ فإن $\phi(d) \mid \phi(n)$.

الحل: لنكتب $n=\prod_{i=1}^{r} p_i^{\alpha_i}$ حيث $\alpha_i \ge 1$ لجميع القيم $1 \le i \le r$. إذا كان $d \mid n$ فإن $d=\prod_{i=1}^{r} p_i^{\beta_i}$ حيث $0 \le \beta_i \le \alpha_i$ لجميع القيم $1 \le i \le r$. هذا يعطي $\phi(n)=\prod_{i=1}^{r} p_i^{\alpha_i-1}(p_i-1)$ و $\phi(d)=\prod_{i=1}^{r} p_i^{\beta_i-1}(p_i-1)$، حيث إنه إذا كان $\beta_i=0$ فإن المقدار $p_i^{\beta_i-1}(p_i-1)$ لن يكون موجوداً في $\phi(d)$. الآن حيث إن $\beta_i \le \alpha_i$ فإننا نستنتج من ذلك أن $\phi(d) \mid \phi(n)$.

مثال 21: صِف جميع الأعداد الصحيحة الموجبة n التي تُحقِق $\phi(n)=\frac{n}{2}$.

الحل: بما أن $n=2\phi(n)$ فإن n عدد زوجي. إذا كان n يقبل القسمة على عدد أولي فردي فإنه يُمكننا أن نكتب

$$n=2^k\cdot\prod_{i=1}^{r}p_i^{\alpha_i},\ \ k\ge 1,\ \alpha_i\ge 1$$

حيث p_i عدد أولي فردي لجميع القيم $1\le i\le r$. بملاحظة أن

$$\phi(n)=2^{k-1}\cdot\prod_{i=1}^{r}p_i^{\alpha_i-1}(p_i-1),\quad \frac{n}{2}=2^{k-1}\cdot\prod_{i=1}^{r}p_i^{\alpha_i}$$

نستنتج أن $2^{k+r-1}\,|\,\phi(n)$ و $2^{k-1}\,\|\,\frac{n}{2}$. حيث إن $k+r-1>k-1$ إذاً $\phi(n)\ne\frac{n}{2}$. هذا يقتضي أن n لا يقبل القسمة على أي عدد أولي فردي، أي أن $n=2^k$ حيث k عدد صحيح موجب. بما أن

$$\phi(2^k)=2^{k-1}=\frac{2^k}{2}$$

إذاً $n=2^k$، حيث k عدد صحيح موجب، هي القيم التي تُحقِق المعادلة $\phi(n)=\frac{n}{2}$.

مثال 22: أثبت أن $55\,|\,n^{20}-1$ لجميع الأعداد الصحيحة n التي تُحقق $(n,55)=1$.

الحل: بما أن $(n,55)=1$ فإن $(n,5)=1$ و $(n,11)=1$. باستخدام نظرية فيرما نحصل على الآتي:

- $n^4\equiv 1 \bmod 5$ ومنه نستنتج أن $n^{20}\equiv 1 \bmod 5$
- $n^{10}\equiv 1 \bmod 11$ ومنه نستنتج أن $n^{20}\equiv 1 \bmod 11$

هذا يقتضي أن $n^{20}\equiv 1 \bmod [5,11]$، أي أن $n^{20}\equiv 1 \bmod 55$ ومن ثم

$55 \mid n^{20}-1$.

مثال 23: إذا كان p عدداً أولياً و a عدداً صحيحاً و $k \geq 1$ عدداً صحيحاً، فأثبت أن $a^{1+k(p-1)} \equiv a \bmod p$.

الحل: إذا كان $(a,p)=p$، أي أن $p \mid a$، فإن $p \mid a^{1+k(p-1)}-a$ ومن ثم $a^{1+k(p-1)} \equiv a \bmod p$. وإذا كان $(a,p)=1$، أي أن $p \nmid a$، فباستخدام نظرية فيرما نحصل على $a^{p-1} \equiv 1 \bmod p$. برفع الطرفين إلى الأس k يصبح لدينا $a^{k(p-1)} \equiv 1 \bmod p$. بضرب الطرفين بالعدد a نحصل على $a^{1+k(p-1)} \equiv a \bmod p$.

مثال 24: أثبت أنه إذا كان $n>4$ عدداً مؤلفاً فإن $(n-1)! \equiv 0 \bmod n$.

الحل: حيث إن n عدد مؤلف فبإمكاننا أن نكتب $n=ab$ حيث $1<a<n$ و $1<b<n$. توجد حالتان محتملتان:

الحالة الأولى: $a \neq b$. في هذه الحالة يكون لدينا $a,b \in \{1,2,\cdots,n-1\}$ ومن ثم $n=ab \mid (n-1)!$ أو $(n-1)! \equiv 0 \bmod n$.

الحالة الثانية: $a=b$. في هذه الحالة $a,2a \in \{1,2,\cdots,n-1\}$ وذلك لأن $a<2a<a^2=n$:

$$n=a^2>4 \Rightarrow a>2 \Rightarrow a-2>0 \Rightarrow a(a-2)>0 \Rightarrow a^2>2a$$

هذا يقتضي أن $2a^2 \mid (n-1)!$ ومن ثم $n=a^2 \mid (n-1)!$، أي أن $(n-1)! \equiv 0 \bmod n$.

مثال 25: ليكن $R_n=\underbrace{111\cdots11}_{n}$ (عدد واحدي- Repunit). أثبت أنه إذا كان $p>5$ عدداً أولياً فإن $p \mid R_{p-1}$.

الحل: بما أن $p>5$ فإن $(p,10)=1$. باستخدام نظرية فيرما نحصل على

$10^{p-1} \equiv 1 \bmod p$، أو $p \mid 10^{p-1}-1$. لكن $10^{p-1}-1 = \underbrace{999\cdots9}_{p-1} = 9\times R_{p-1}$ و $(p,9)=1$، إذاً $p \mid R_{p-1}$.

تعريف 10.

1. نقول إنَّ العدد المؤلف n **عدد شبه أولي** (Pseudoprime number) للأساس b إذا كان $(n,b)=1$ و $b^{n-1} \equiv 1 \bmod n$.
2. نقول إنَّ العدد المؤلف n **عدد كارمايكل** (Carmichael number) إذا كان $b^{n-1} \equiv 1 \bmod n$ لأي عدد صحيح b حيث $(b,n)=1$.

مثال 26: العدد 15 هو عدد شبه أولي للأساس 4: بما أن $4^2 \equiv 1 \bmod 15$ فإن $4^{14} \equiv 1 \bmod 15$.

مثال 27: العدد 1105 هو عدد كارمايكل: لاحظ أولاً أن $1105 = 5\times13\times17$ و $1104 = 16\times3\times23$. ليكن a عدداً صحيحاً بحيث $(a,1105)=1$. إذاً $(a,5)=(a,13)=(a,17)=1$. باستخدام نظرية فيرما نحصل على الآتي:

$$a^4 \equiv 1 \bmod 5 \Rightarrow a^{1104} \equiv 1 \bmod 5$$
$$a^{12} \equiv 1 \bmod 13 \Rightarrow a^{1104} \equiv 1 \bmod 13$$
$$a^{16} \equiv 1 \bmod 17 \Rightarrow a^{1104} \equiv 1 \bmod 17$$

هذا بدوره يقتضي أنَّ $a^{1104} \equiv 1 \bmod [5,13,17]$، أي أن $a^{1104} \equiv 1 \bmod 1105$.

حل التطابقات

لتكن $f(x)$ كثيرة حدود معاملاتها أعداد صحيحة. نقول إن العدد الصحيح a حلٌ للتطابق

$$f(x)\equiv 0 \bmod m$$

إذا كان $f(a)\equiv 0 \bmod m$. إذا كان $b\equiv a \bmod m$، فإن $f(b)\equiv f(a)\equiv 0 \bmod m$ ومن ثم فإن b حلٌ آخر للتطابق أعلاه. في هذه الحالة ننظر لجميع الأعداد المطابقة للعدد a قياس m كحلٍ واحدٍ و نقول إن $x\equiv a \bmod m$ هو حلٌ للتطابق المعطى أعلاه.

تعريف 11.

ليكن $\{c_1,c_2,\cdots,c_m\}$ نظام رواسب تام قياس m. عدد الحلول للتطابق $f(x)\equiv 0 \bmod m$ يساوي عدد الأعداد c_i التي تحقق $f(c_i)\equiv 0 \bmod m$.

مثال 28: باستخدام نظام الرواسب التام قياس 5: $\{0,1,2,3,4\}$ نلاحظ الآتي:

أ. لا يوجد للتطابق $x^2-3\equiv 0 \bmod 5$ أي حل.

ب. يوجد للتطابق $x^3-2x+1\equiv 0 \bmod 5$ حلان هما $x\equiv 1,2 \bmod 5$.

ج. يوجد للتطابق $x^5-x\equiv 0 \bmod 5$ خمسة حلول هي $x\equiv 0,1,2,3,4 \bmod 5$.

التطابقات الخطية (Linear Congruences)

نظرية 23.

ليكن $(a,m)=g$. التطابق الخطي $ax\equiv b \bmod m$ قابل للحل إذا و فقط إذا كان $g\,|\,b$. عند تحقق هذا الشرط، يكون للتطابق $ax\equiv b \bmod m$ عدد g من الحلول قياس m:

$$x \equiv x_0, x_0 + \frac{m}{g}, x_0 + \frac{2m}{g}, \cdots, x_0 + \frac{(g-1)m}{g} \mod g$$

حيث x_0 هو الحل الوحيد قياس $\frac{m}{g}$ للتطابق الخطي $\frac{a}{g}x \equiv \frac{b}{g} \mod \frac{m}{g}$.

مثال 29: حيث إن $(5,7)=1$ فإن للتطابق الخطي $5x \equiv 1 \mod 7$ حلاً واحداً قياس 7. بملاحظة أن

$$5x \equiv 1 \equiv 8 \equiv 15 \mod 7$$

فإنه بالقسمة على 5 نحصل على الحل $x \equiv 3 \mod 7$.

مثال 30: بما أن $(6,15)=3$ فإن للتطابق $6x \equiv 9 \mod 15$ ثلاث حلول قياس 15. بالتقسيم على 3 نحصل على التطابق $2x \equiv 3 \mod 5$. لكن $2x \equiv 3 \equiv 8 \mod 5$ يقتضي أن $x \equiv 4 \mod 5$، ومنه نستنتج أن الحلول قياس 15 هي $x \equiv 4,9,14 \mod 15$.

نظرية 24. (نظرية الباقي الصينية- ***Chinese Remainder Theorem***)

ليكن $m_1, m_2, \cdots, m_r$ أعداداً صحيحة موجبة أولية نسبياً مثنى مثنى، وليكن $a_1, a_2, \cdots, a_r$ أعداداً صحيحة. إذاً يوجد لنظام التطابقات

$$\begin{aligned} x &\equiv a_1 \mod m_1 \\ x &\equiv a_2 \mod m_2 \\ &\vdots \\ x &\equiv a_r \mod m_r \end{aligned}$$

حلٌ واحدٌ قياس $m_1 m_2 \cdots m_r$.

مثال 32: حيث إن $(3,5)=1$ فإن للنظام

$$\begin{cases} x \equiv 1 \bmod 3 \\ x \equiv 2 \bmod 5 \end{cases}$$

حل وحيد قياس 15. التطابق الأول يقتضي أن $x = 1+3k$ حيث k عدد صحيح. بالتعويض في التطابق الثاني نحصل على $1+3k \equiv 2 \bmod 5$ أو $3k \equiv 1 \equiv 6 \bmod 5$ ومن ثم $k \equiv 2 \bmod 5$. هذا يعني أن $k = 2+5l$ حيث l عدد صحيح. إذاً $x = 1+3k = 1+3(2+5l) = 7+15l$، أي أن حل النظام هو $x \equiv 7 \bmod 15$.

مثال 33: لحل النظام

$$\begin{cases} x \equiv 4 \bmod 6 \\ x \equiv 3 \bmod 10 \end{cases}$$

نكتب أولاً التطابق الأول على الصيغة $x = 4+6k$، حيث k عدد صحيح. بالتعويض في التطابق الثاني نحصل على $4+6k \equiv 3 \bmod 10$ أو $6k \equiv -1 \equiv 9 \bmod 10$. بما أن $(6,10) = 2$ لا يقسم العدد 9 فإنه لا يوجد k يُحقق التطابق. نستنتج من ذلك أنه لا يوجد حل للنظام المعطى.

طريقة حل التطابق $f(x) \equiv 0 \bmod m$

ليكن $m = p_1^{\alpha_1} \times p_2^{\alpha_2} \times \cdots \times p_r^{\alpha_r}$. العدد a يُحقق التطابق

$$f(x) \equiv 0 \bmod m \text{.............}(1)$$

إذا وفقط إذا كان العدد a يُحقق نظام التطابقات

$$\begin{aligned} &f(x) \equiv 0 \bmod p_1^{\alpha_1} \\ &f(x) \equiv 0 \bmod p_2^{\alpha_2} \text{.............}(2) \\ &\vdots \\ &f(x) \equiv 0 \bmod p_r^{\alpha_r} \end{aligned}$$

نستنتج من ذلك أنه لحل التطابق (1) نقوم أولاً بحل كل تطابق في النظام (2). ثم نُكوِّن أنظمة تطابقات، كلٌ منها مُكوَّن من عدد r من التطابقات الخطية. كل نظام يتكون من حلٍّ واحد من حلول كل تطابق في (2). نقوم بحل كل نظام مُكوَّن باستخدام نظرية الباقي الصينية. الحلول الناتجة هي حلول التطابق (1).

مثال 34: جِد حلول التطابق $x^3+2x+3\equiv 0 \bmod 55$.

الحل: التطابق المعطى يكافئ النظام الآتي:

$$\begin{cases} x^3+2x+3\equiv 0 \bmod 5 \\ x^3+2x+3\equiv 0 \bmod 11 \end{cases}$$

حلول التطابق الأول هي $x\equiv -1 \bmod 5$ و $x\equiv 2 \bmod 5$. أما حلول التطابق الثاني فهي $x\equiv -1 \bmod 11$ و $x\equiv -5 \bmod 11$. هذه الحلول تُعطينا أربعة أنظمة خطية:

$$\begin{cases} x\equiv -1 \bmod 5,\ x\equiv -1 \bmod 11 \\ x\equiv -1 \bmod 5,\ x\equiv -5 \bmod 11 \\ x\equiv 2 \bmod 5,\ x\equiv -1 \bmod 11 \\ x\equiv 2 \bmod 5,\ x\equiv -5 \bmod 11 \end{cases}$$

حلول هذه الأنظمة هي على التوالي $x\equiv -1 \bmod 55$، $x\equiv 39 \bmod 55$، $x\equiv 32 \bmod 55$، $x\equiv 17 \bmod 55$ وهي تُمثل حلول التطابق المعطى.

أعداد فيرما و أعداد مِرسان (Fermat Numbers and Mersenne Numbers)

تعريف 12.

1. لأي عدد صحيح $n \geq 0$، **عدد فيرما** هو العدد $F_n = 2^{2^n} + 1$.
2. لأي عدد صحيح $n \geq 1$، **عدد مِرسان** هو العدد $M_n = 2^n - 1$.

مثال 35: أثبت أن $(F_n, F_m) = 1$ لأي عددين $n \neq m$.

الحل: يمكننا أن نفرض أولاً أن $n > m$. باستخدام المُتطابقة $a^2 - 1 = (a-1)(a+1)$ بشكلٍ مُتكرر نحصل على ما يأتي:

$$F_n - 2 = 2^{2^n} - 1 = F_{n-1}F_{n-2}\cdots F_1F_0$$

هذا يقتضي أن $(F_n, F_m) \mid 2$، أي أن $(F_n, F_m) = 1$ أو $(F_n, F_m) = 2$. بما أن أعداد فيرما أعداد فردية فإننا نستنتج أن $(F_n, F_m) = 1$.

مثال 36: أثبت أنه إذا كان $n \geq 2$ فإن $F_n \equiv 7 \bmod 10$.

الحل: نلاحظ – أولاً– ما يأتي:

- $2^{2^n} \equiv 0 \bmod 2$ ومن ثم $F_n = 2^{2^n} + 1 \equiv 1 \bmod 2$.
- $2^{2^n} = 4^{2^{n-1}} \equiv (-1)^{2^{n-1}} \equiv 1 \bmod 5$ ومن ثم $F_n \equiv 2 \bmod 5$.

بوضع $x = F_n$ وحل نظام التطابقات $x \equiv 1 \bmod 2$، $x \equiv 2 \bmod 5$ نجد أن الحل هو $x \equiv 7 \bmod 10$. إذاً $F_n \equiv 7 \bmod 10$.

مثال 37: أثبت أن $(M_n, M_{n+1}) = 1$ لجميع القيم $n \geq 1$.

الحل: الإثبات ينتج مباشرة من العلاقة $M_{n+1} = 2M_n + 1$.

مثال 38: أثبت أنه إذا كان $1 \leq k < n$ فإن $M_n = 2^k M_{n-k} + M_k$.

الحل: الإثبات ينتج من الآتي:

$$\begin{aligned} M_n &= 2^n - 1 \\ &= 2^{n-k+k} - 2^k + 2^k - 1 \\ &= 2^k(2^{n-k} - 1) + (2^k - 1) \\ &= 2^k M_{n-k} + M_k \end{aligned}$$

مثال 39: ليكن p عدداً أولياً. أثبت أنه إذا كان عدد مِرسان $M_p = 2^p - 1$ عدداً مؤلفاً فإن M_p عدد شبه أولي للأساس 2.

الحل: نريد أن نثبت أن $2^{M_p - 1} \equiv 1 \bmod M_p$. بما أن p عدد أولي فردي، فباستخدام نظرية فيرما نحصل على

$$M_p - 1 = 2^p - 2 = 2(2^{p-1} - 1) \equiv 0 \bmod p$$

أي أن $M_p - 1 = kp$، حيث k عدد صحيح موجب. لكن $2^p \equiv 1 \bmod M_p$. برفع طرفي التطابق السابق إلى الأس k نحصل على $2^{M_p - 1} \equiv 1 \bmod M_p$ وهو المطلوب.

الجذور البدائية (Primitive Roots)

تعريف 13.

ليكن a عدداً صحيحاً و $m > 1$ عدداً صحيحاً موجباً بحيث $(a,m) = 1$. نقول إنَّ العدد h هو رُتبة العدد a قياس m إذا كان العدد h هو أصغر عدد صحيح موجب يُحقق $a^h \equiv 1 \bmod m$. في هذه الحالة نكتب $\mathrm{ord}_m(a) = h$.

مثال 40:

أ- رتبة العدد 4 قياس 15 تساوي 2 لأن $4^1 \equiv 4 \bmod 15$، $4^2 \equiv 1 \bmod 15$.

ب- رتبة العدد 2 قياس 5 تساوي 4 لأن
$2^1 \equiv 2,\ 2^2 \equiv 4,\ 2^3 \equiv 3,\ 2^4 \equiv 1 \bmod 5$.

نظرية 25.

1. إذا كان $\text{ord}_m(a) = h$ و k عدد صحيح موجب، فإن $a^k \equiv 1 \bmod m$ إذا وفقط إذا كان $h \mid k$.
2. إذا كان $\text{ord}_m(a) = h$ فإن $h \mid \phi(m)$.
3. إذا كان $\text{ord}_m(a) = h$ فإن $\text{ord}_m(a^k) = \dfrac{h}{(h,k)}$.
4. إذا كان $\text{ord}_m(a) = h$ فإن $a^r \equiv a^s \bmod m$ إذا وفقط إذا كان $r \equiv s \bmod h$.
5. إذا كان $\text{ord}_m(a) = h$ فإن أي عددين من الأعداد $a,\ a^2, \ldots, a^h$ غير مطابقين قياس m.
6. إذا كان $\text{ord}_m(a) = h$ و $\text{ord}_m(b) = k$ و $(h,k) = 1$، فإن $\text{ord}_m(ab) = hk$.

مثال 41: أثبت أنه إذا كان $\text{ord}_n(a) = n-1$ فإن n عدد أولي.

الحل: من الفقرة الثانية من نظرية 25 نجد أن $n-1 \mid \phi(n)$ ومن ثم $n-1 \le \phi(n)$. لكن من تعريف دالة أويلر نجد أيضاً أن $\phi(n) \le n-1$. هذا يقتضي أن $\phi(n) = n-1$. باستخدام مثال 19 نستنتج أن n عدد أولي.

تعريف 14.

ليكن g عدداً صحيحاً و $m > 1$ عدداً صحيحاً موجباً بحيث $(g,m) = 1$. إذا كان $\text{ord}_m(g) = \phi(m)$ فإن العدد g يُسمى جذراً

بدائياً قياس m.

مثال 42:

أ- العدد 3 جذر بدائي قياس 10 لأن $\phi(10)=4$ و

$3^1 \equiv 3,\ 3^2 \equiv 9,\ 3^3 \equiv 7,\ 3^4 \equiv 1 \bmod 10$.

ب- العدد 3 جذر بدائي قياس 7 لأن $\phi(7)=6$ و

$$3^1 \equiv 3,\ 3^2 \equiv 2,\ 3^3 \equiv 6,\ 3^4 \equiv 4,\ 3^5 \equiv 5,\ 3^6 \equiv 1 \bmod 7$$

ملحوظة: لبعض الأعداد الصحيحة الموجبة m لا يوجد أي جذر بدائي قياس m. أنظر على سبيل المثال السؤال رقم 137.

نظرية 26.

إذا كان g جذراً بدائياً قياس $m>1$ فإن مجموعة الأعداد $g, g^2, g^3, \cdots, g^{\phi(m)}$ تُمثِّل نظام رواسب مختزَل قياس m.

نظرية 27.

إذا كان p عدداً أولياً فإنه يوجد $\phi(p-1)$ جذر بدائي قياس p.

الرواسب التربيعية (Quadratic Residues)

تعريف 15.

ليكن a و $m>1$ عددين صحيحين بحيث إنَّ $(a,m)=1$. نقول إنَّ العدد a **راسب تربيعي قياس** m إذا كان التطابق $x^2 \equiv a \bmod m$ قابل للحل. إذا لم بوجد أي حل للتطابق $x^2 \equiv a \bmod m$ فإننا نقول إنَّ العدد a **راسب غير تربيعي قياس** m.

مثال 43:

أ- العدد 2 راسب تربيعي قياس 7 لأن التطابق $x^2 \equiv 2 \bmod 7$ قابل للحل: حلوله هي $x \equiv 3,4 \bmod 7$.

ب- العدد 3 راسب غير تربيعي قياس 7 لأنه لا يوجد أي حل للتطابق $x^2 \equiv 3 \bmod 7$.

نظرية 28.

ليكن p عدداً أولياً فردياً و a عددا صحيحاً.

1. التطابق $x^2 \equiv a \bmod p$ إما أن يكون غير قابل للحل أو يوجد له حلان. إذا كان $x \equiv x_0 \bmod p$ حلاً للتطابق فإن الحل الآخَر هو $x \equiv -x_0 \bmod p$.

2. يوجد $\frac{p-1}{2}$ راسب تربيعي قياس p و $\frac{p-1}{2}$ راسب غير تربيعي قياس p. الرواسب التربيعية قياس p هي مطابقة قياس p للأعداد

$$1^2, 2^2, 3^2, \cdots, \left(\frac{p-1}{2}\right)^2$$

مثال 44: حيث إنَّ

$$1^2, 2^2, 3^2, 4^2, 5^2, 6^2 \equiv 1,4,9,3,12,10 \bmod 13$$

فإن الرواسب التربيعية قياس 13 هي 1,3,4,9,10,12 ومن ثم فإن الرواسب غير التربيعية قياس 13 هي 2,5,6,7,8,11.

تعريف 16. (رمز ليجيندر -*Legendre's Symbol*)

ليكن a عدداً صحيحاً و p عدداً أولياً فردياً. رمز ليجيندر $\left(\frac{a}{p}\right)$

مُعَرف كما يأتي:

$\left(\frac{a}{p}\right)=1$ إذا كان a راسباً تربيعياً قياس p و $\left(\frac{a}{p}\right)=-1$ إذا كان a راسباً غير تربيعي قياس p و $\left(\frac{a}{p}\right)=0$ إذا كان $p|a$.

نظرية 29.

ليكن a و b عددين صحيحين و p عدداً أولياً فردياً.

1. $\left(\frac{a}{p}\right)\equiv a^{(p-1)/2} \bmod p$
2. $\left(\frac{a}{p}\right)\left(\frac{b}{p}\right)=\left(\frac{ab}{p}\right)$
3. إذا كان $a\equiv b \bmod p$ فإن $\left(\frac{a}{p}\right)=\left(\frac{b}{p}\right)$
4. إذا كان $(a,p)=1$ فإن $\left(\frac{a^2}{p}\right)=1$
5. $\left(\frac{-1}{p}\right)=(-1)^{\frac{p-1}{2}}$
6. $\left(\frac{2}{p}\right)=(-1)^{\frac{p^2-1}{8}}$

ملحوظة: من الفقرتين الخامسة والسادسة من النظرية السابقة نستنتج الآتي:

1. إذا كان $p\equiv 1 \bmod 4$ فإن $\left(\frac{-1}{p}\right)=1$ وإذا كان $p\equiv 3 \bmod 4$ فـإن $\left(\frac{-1}{p}\right)=-1$.

2. إذا كان $p \equiv 1,\ 7 \bmod 8$ فإن $\left(\frac{2}{p}\right)=1$ وإذا كان $p \equiv 3,\ 5 \bmod 8$ فإن $\left(\frac{2}{p}\right)=-1$.

نظرية 30. (قانون جاوس للمقلوبية ***Gauss's Quadratic Reciprocity Law***)

إذا كان p و q عددين أوليين فرديين مختلفين فإن

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right)=(-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}$$

ملحوظة: من قانون جاوس للمقلوبية نستنتج الآتي:

1. إذا كان $p \equiv 1 \bmod 4$ أو $q \equiv 1 \bmod 4$ فإن $\left(\frac{p}{q}\right)=\left(\frac{q}{p}\right)$.
2. إذا كان $p \equiv 3 \bmod 4$ و $q \equiv 3 \bmod 4$ فإن $\left(\frac{p}{q}\right)=-\left(\frac{q}{p}\right)$.

مثال 45: هل توجد حلول للتطابق $x^2 \equiv -1 \bmod 97$. (العدد 97 عدد أولي)

الحل: بما أن $\left(\frac{-1}{97}\right)=(-1)^{\frac{97-1}{2}}=1$، إذاً التطابق المعطى قابل للحل.

مثال 46: ليكن p عدداً أولياً فردياً و $(a,p)=(b,p)=1$. أثبت أنه إذا كان التطابق $x^2 \equiv a \bmod p$ قابل للحل و التطابق $x^2 \equiv b \bmod p$ غير قابل للحل، فإن التطابق $x^2 \equiv ab \bmod p$ غير قابل للحل.

الحل: نقوم بحساب $\left(\frac{ab}{p}\right)$. من معطيات السؤال، نجد أن $\left(\frac{a}{p}\right)=1$ و $\left(\frac{b}{p}\right)=-1$. هذا يقتضي أن $\left(\frac{ab}{p}\right)=\left(\frac{a}{p}\right)\left(\frac{b}{p}\right)=(1)(-1)=-1$ ومن

ثم فالتطابق $x^2 \equiv ab \mod p$ غير قابل للحل.

مثال 47: احسب قيمة $\left(\frac{17}{97}\right)$.

الحل: باستخدام النظريتين السابقتين نجد أن

$$\left(\frac{17}{97}\right)=(-1)^{\frac{17-1}{2}\cdot\frac{97-1}{2}}\left(\frac{97}{17}\right)=\left(\frac{12}{17}\right)=\left(\frac{4}{17}\right)\left(\frac{3}{17}\right)$$
$$=\left(\frac{3}{17}\right)=(-1)^{\frac{3-1}{2}\cdot\frac{17-1}{2}}\left(\frac{17}{3}\right)=-\left(\frac{2}{3}\right)$$
$$=-(-1)^{\frac{9-1}{8}}=1$$

مثال 48: جِد جميع الأعداد الأولية $p>2$ التي تُحقِق $\left(\frac{5}{p}\right)=1$.

الحل: باستخدام قانون جاوس للمقلوبية نجد أن

$$\left(\frac{5}{p}\right)=(-1)^{\frac{p-1}{2}\cdot\frac{5-1}{2}}\left(\frac{p}{5}\right)=\left(\frac{p}{5}\right)$$

حيث إنَّ $p\equiv 1,\ 2,\ 3,\ 4 \mod 5$ فإنه سيصبح لدينا الاحتمالات الآتية:

$$\left(\frac{p}{5}\right)=\left(\frac{1}{5}\right)=1$$
$$\left(\frac{p}{5}\right)=\left(\frac{2}{5}\right)=(-1)^{\frac{5^2-1}{8}}=-1$$
$$\left(\frac{p}{5}\right)=\left(\frac{3}{5}\right)=(-1)^{\frac{3-1}{2}\cdot\frac{5-1}{2}}\left(\frac{5}{3}\right)=\left(\frac{2}{3}\right)=(-1)^{\frac{3^2-1}{8}}=-1$$
$$\left(\frac{p}{5}\right)=\left(\frac{4}{5}\right)=1$$

هذا يقتضي أن $\left(\frac{5}{p}\right)=1$ إذا وفقط إذا كان $p\equiv 1,\ 4 \bmod 5$.

مثال 49: أثبت أنه يوجد عدد غير منتهٍ من الأعداد الأولية ذات الشكل العام $4n+1$.

الحل: نُثبت أنه لأي عدد صحيح $m\geq 1$ يوجد عدد أولي $p\equiv 1 \bmod 4$ أكبر من m . هذا سوف يقتضي وجود عدد غير منتهٍ من الأعداد الأولية ذات الشكل العام $4n+1$.

ليكن $m\geq 1$ عدداً صحيحاً. لِنضع $A=(m!)^2+4$. إذا كان $p>2$ عدداً أولياً بحيث $p\mid A$ ، فإن $p>m$ لأنه لو كان $p\leq m$ فإن $p\mid 4$ وهذا مُستحيل. نستنتج من ذلك أن $(p,m!)=1$. حيث إن $p\mid A$ فإن $(m!)^2\equiv -4 \bmod p$. هذا يقتضي أن

$$1=\left(\frac{(m!)^2}{p}\right)=\left(\frac{-4}{p}\right)=\left(\frac{-1}{p}\right)\left(\frac{4}{p}\right)=\left(\frac{-1}{p}\right)$$

ومن ثم $p\equiv 1 \bmod 4$. وبهذا يتم الإثبات.

الدوال العددية (Arithmetic Functions)

تعريف 17. (دالة الصحيح – *Greatest Integer Function*)

إذا كان x عدداً حقيقياً فإن $[\![x]\!]$ يُعرف كأكبر عدد صحيح أقلٍ من أو يساوي x . الرمز $[\![x]\!]$ يُقرأ "صحيح x". (مثلاً: $[\![3.27]\!]=3$ ، $[\![-3.27]\!]=-4$ ، $[\![5]\!]=5$)

نظرية 31.

1. لأي عدد حقيقي x ، $x-1<[\![x]\!]\leq x$.

2. لأي عدد صحيح m، $[\![x+m]\!]=[\![x]\!]+m$.

3. لأي عدد صحيح موجب m، $\left[\!\!\left[\frac{x}{m}\right]\!\!\right]=\left[\!\!\left[\frac{[\![x]\!]}{m}\right]\!\!\right]$.

4. إذا كان x و y عددين حقيقيين فإن $[\![x+y]\!]\leq[\![x]\!]+[\![y]\!]$.

5. إذا كان a و n عددين صحيحين موجبين فإن عدد الأرقام القابلة للقسمة على a من ضمن الأرقام $1,2,3,\cdots,n$ يساوي $\left[\!\!\left[\frac{n}{a}\right]\!\!\right]$.

مثال 50: إذا كان $x>0$ عدداً حقيقياً غير صحيح فأثبت أن $[\![-x]\!]=-[\![x]\!]-1$.

الحل: بكتابة x على الشكل $x=[\![x]\!]+\theta$ حيث $0<\theta<1$، نجد أن

$$-x=-[\![x]\!]-1+(1-\theta)$$

بما أن $0<1-\theta<1$ و $-[\![-x]\!]-1$ عدد صحيح، فباستخدام الخاصية 2 من نظرية 31 نجد أنّ

$$[\![-x]\!]=-[\![-x]\!]-1+[\![1-\theta]\!]=-[\![-x]\!]-1+0=-[\![-x]\!]-1$$

نظرية 32.

ليكن p عدداً أولياً. إن أكبر أُس e_p بحيث أن $p^{e_p}\mid n!$ يساوي

$$e_p=\sum_{i=1}^{\infty}\left[\!\!\left[\frac{n}{p^i}\right]\!\!\right]$$

مثال 51: أكبر أُس e_3 بحيث $3^{e_3}\mid 122!$ يساوي

$$e_3=\sum_{i=1}^{\infty}\left[\!\!\left[\frac{122}{3^i}\right]\!\!\right]$$

لإجراء الحسابات نستخدم الخاصية 3 من نظرية 31 أعلاه:

$$\left[\!\left[\frac{122}{3}\right]\!\right]=40$$

$$\left[\!\left[\frac{122}{3^2}\right]\!\right]=\left[\!\left[\frac{[\![122/3]\!]}{3}\right]\!\right]=\left[\!\left[\frac{40}{3}\right]\!\right]=13$$

$$\left[\!\left[\frac{122}{3^3}\right]\!\right]=\left[\!\left[\frac{[\![122/3^2]\!]}{3}\right]\!\right]=\left[\!\left[\frac{13}{3}\right]\!\right]=4$$

$$\left[\!\left[\frac{122}{3^4}\right]\!\right]=\left[\!\left[\frac{[\![122/3^3]\!]}{3}\right]\!\right]=\left[\!\left[\frac{4}{3}\right]\!\right]=1$$

$$\left[\!\left[\frac{122}{3^5}\right]\!\right]=\left[\!\left[\frac{[\![122/3^4]\!]}{3}\right]\!\right]=\left[\!\left[\frac{1}{3}\right]\!\right]=0$$

إذاً $e_3 = 40+13+4+1=58$.

تعريف 18.

ليكن n عدداً صحيحاً موجباً. نقوم بتعريف الدوال الآتية:

1. $\tau(n)$ هو عدد القواسم الموجبة للعدد n.
2. $\sigma(n)$ هو مجموع القواسم الموجبة للعدد n.
3. $\omega(n)$ هو عدد الأعداد الأولية المختلفة التي تقسم العدد n إذا كان $n>1$، و $\omega(1)=1$.

مثال 52: القواسم الموجبة للعدد $75=3\cdot 5^2$ هي $1,3,5,15,25,75$. إذاً $\tau(75)=6$ ، $\sigma(75)=124$ ، $\omega(75)=2$.

نظرية 33.

إذا كان $n=p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_r^{\alpha_r}$ (تحليل n إلى عوامله الأولية)، فإن

$$\tau(n)=(\alpha_1+1)(\alpha_2+1)\cdots(\alpha_r+1)$$
$$\sigma(n)=\frac{p_1^{\alpha_1+1}-1}{p_1-1}\cdot\frac{p_2^{\alpha_2+1}-1}{p_2-1}\cdots\cdots\frac{p_r^{\alpha_r+1}-1}{p_r-1}$$
$$\omega(n)=r$$

الدوال المعرفة أعلاه هي أمثلة لما يُسمى بالدوال العددية التي نعرفها كما يأتي.

تعريف19.

1. نقول إنَّ الدالة f **دالة عددية** إذا كان مجالها مجموعة الأعداد الصحيحة الموجبة.
2. نقول إنَّ الدالة العددية f (حيث f دالة غير صفرية) **دالة ضربية** (Multiplicative Function) إذا كان $f(mn)=f(m)f(n)$ لأي عددين صحيحين موجبين m و n يحققان $(m,n)=1$.

نظرية 34.

الدوال العددية $\omega,\ \sigma,\ \tau$ هي دوال ضربية.

نظرية 35.

إذا كانت f دالة ضربية و $F(n)=\sum_{d|n}f(d)$ فإن F دالة ضربية.

مثال 53: أثبت أن $\tau(n)$ عدد فردي إذا و فقط إذا كان n مربعاً كاملاً.

الحل: لنكتب $n=\prod_{i=1}^{r}p_i^{\alpha_i}$. إذاً $\tau(n)=\prod_{i=1}^{r}(\alpha_i+1)$. إذا كان $\tau(n)$ عدداً فردياً فإن α_i+1 عدد فردي لجميع القيم $1\le i\le r$. هذا يعني أن α_i عدد زوجي لجميع القيم $1\le i\le r$. لو كتبنا $\alpha_i=2\beta_i$، نحصل على

$n=\prod_{i=1}^{r}p_i^{2\beta_i}=\left(\prod_{i=1}^{r}p_i^{\beta_i}\right)^2$، أي أن n مربع كامل. إذا كان n مربعاً كاملاً فيمكننا أن نكتب $n=\prod_{i=1}^{r}p_i^{2\beta_i}$ ومن ثم $\tau(n)=\prod_{i=1}^{r}(2\beta_i+1)$ عدد فردي.

تعريف 20. (دالة موبيوس -*Möbius Function*)

دالة موبيوس μ هي الدالة العددية المعرفة كمايلي: إذا كان $n=p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_r^{\alpha_r}$، فإن $\mu(1)=1$، $\mu(n)=0$ إذا كان $\alpha_i\geq 2$ لقيمة ما i، و $\mu(n)=(-1)^r$ إذا كان $\alpha_1=\alpha_2=\cdots=\alpha_r=1$.

نظرية 36.

دالة موبيوس μ هي دالة ضربية، وإذا كان $n>1$ فإن $\sum_{d|n}\mu(d)=0$.

نظرية 37. (صيغة موبيوس العكسية -*Möbius Inversion Formula*)

إذا كان $F(n)=\sum_{d|n}f(d)$ لأي عدد صحيح موجب n فإن $f(n)=\sum_{d|n}\mu(d)F(n/d)$.

مثال 54:

أ- حيث إن $\tau(n)=\sum_{d|n}1$ فإنه باستخدام صيغة موبيوس العكسية مع $f(n)=1$ و $F(n)=\tau(n)$ نحصل على $1=\sum_{d|n}\mu(d)\tau(n/d)$.

ب- حيث إن $\sigma(n)=\sum_{d|n} d$ فإنه باستخدام صيغة موبيوس العكسية مع $f(n)=n$ و $F(n)=\sigma(n)$ نحصل على
$n=\sum_{d|n}\mu(d)\sigma(n/d)$.

مثال 55: جِد قيمة المجموع $\sum_{d|n} d\,\mu(d)$ إذا كان $n>1$.

الحل: لنضع $F(n)=\sum_{d|n} d\,\mu(d)$. بما أن $f(n)=n\mu(n)$ دالة ضربية فإننا نستنتج من نظرية 35 أن F دالة ضربية. لِذا نبدأ بإيجاد قيمة $F(p^{\alpha})$ حيث p عدد أولي و $\alpha \geq 1$ عدد صحيح:

$$F(p^{\alpha})=\sum_{d|p^{\alpha}} d\,\mu(d)=\mu(1)+p\,\mu(p)=1-p$$

الآن إذا كان $n=\prod_{i=1}^{r} p_i^{\alpha_i}$ فبسبب أن F دالة ضربية نحصل على

$$F(n)=\prod_{i=1}^{r} F(p_i^{\alpha_i})=\prod_{i=1}^{r}(1-p_i)$$

أي أنَّ

$$\sum_{d|n} d\,\mu(d)=\prod_{p|n}(1-p).$$

تعريف 21. (الأعداد التامة)

نقول إنَّ العدد الصحيح $n \geq 1$ **عدد تام** (Perfect number) إذا كان $\sigma(n)=2n$، **وعدد زائد** (Abundant number) إذا كان $\sigma(n)>2n$، **وعدد ناقص** (Deficient number) إذا كان $\sigma(n)<2n$.

نظرية 38.

العدد الزوجي n عدد تام إذا و فقط إذا كان $n=2^{p-1}(2^{p}-1)$، حيث p و $2^{p}-1$ عددان أوليان.

مثال 56: الأعداد التامة الزوجية الأولى هي 6، 28، 496، 8128، 33550336، 8589869056.

مثال 57: أثبت أن العدد p^k عدد ناقص لأي عدد أولي p وعدد صحيح $k \geq 1$.

الحل: إذا كان $p = 2$ فإن

$$\sigma(2^k) = 2^{k+1} - 1 < 2^{k+1} = 2 \times 2^k$$

ومن ثم فإن العدد 2^k عدد ناقص. لنفرض الآن أن $p > 2$. في هذه الحالة يصبح لدينا الآتي:

$$\sigma(p^k) = \frac{p^{k+1} - 1}{p - 1} = \frac{p^{k+1}(1 - p^{-(k+1)})}{p(1 - p^{-1})} = p^k \frac{1 - p^{-(k+1)}}{1 - p^{-1}}$$

بما أن $1 - p^{-(k+1)} < 1$ و

$$p > 2 \Rightarrow \frac{1}{p} < \frac{1}{2} \Rightarrow 1 - \frac{1}{p} > 1 - \frac{1}{2} = \frac{1}{2} \Rightarrow \frac{1}{(1 - p^{-1})} < 2$$

فإننا نستنتج أن

$$\sigma(p^k) = p^k \frac{1 - p^{-(k+1)}}{1 - p^{-1}} < 2p^k$$

ومن ثم فإن العدد p^k عدد ناقص.

ثلاثيات فيثاغورس (Pythagorean Triples)

في أي مثلث قائم الزاوية مربع طول الوتر يساوي مجموع مربعي طولي الضلعين الآخرين. إذا كان z طول الوتر و x و y طولي الضلعين الآخرين فإن

$$x^2 + y^2 = z^2$$

هذه المعادلة تُسمى **معادلة فيثاغورس**. في حالة كون أطوال الأضلاع أعداداً صحيحة موجبة فإننا نستخدم المصطلحات الآتية:

تعريف 22.

1. **مثلث فيثاغورس** (Pythagorean triangle) هو أي مثلث قائم الزاوية أطوال أضلاعه أعداد صحيحة موجبة.
2. **ثُلاثي فيثاغورس** (Pythagorean triple) هو أي ثلاثي مرتب (x, y, z) مُكوَّن من أعداد صحيحة موجبة يحقق معادلة فيثاغورس $x^2 + y^2 = z^2$.
3. ثلاثي فيثاغورس (x, y, z) يُسمى **ثُلاثي بِدائي** (Primitive triple) إذا كان $(x, y, z) = 1$، أي أنه لا يوجد أي عامل مشترك (أكبر من 1) بين أطوال أضلاعه.

نظرية 39.

جميع ثلاثيات فيثاغورس البدائية (x, y, z) التي فيها y عدد زوجي معطاة كالآتي:

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

حيث r و s عددان صحيحان موجبان أحدهما فردي والآخر زوجي، و $r > s$، و $(r, s) = 1$.

ملحوظة: من الجدير بالذكر أنه في ثلاثية فيثاغورس البدائية (x, y, z) نلاحظ أن أحد العددين x أو y فردي و الآخر زوجي. من دون فقدان التعميم افترضنا في النظرية أعلاه أن y عدد زوجي.

نتيجة 40.

جميع الحلول الصحيحة الموجبة (x,y,z) التي فيها y عدد زوجي لمعادلة فيثاغورس

$$x^2+y^2=z^2$$

مُعطاة كالآتي:

$$\begin{aligned} x &= k(r^2-s^2) \\ y &= 2krs \\ z &= k(r^2+s^2) \end{aligned}$$

حيث k عدد صحيح موجب، و r و s عددان صحيحان موجبان أحدهما فردي والآخر زوجي، و $r>s$، و $(r,s)=1$.

مثال 58: أثبت أنه إذا كان (x,y,z) ثلاثي فيثاغورس بدائي فإنه إما $5|x$ أو $5|y$ أو $5|z$.

الحل: باستخدام نظرية 39 يصبح لدينا

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

حيث r و s عددان صحيحان موجبان أحدهما فردي والآخر زوجي، و $r>s$، و $(r,s)=1$. إذا كان 5 يقسم r أو s فإن $5|y$. لنفرض أن 5 لا يقسم r و s. لاحظ أولاً أن $r^2\equiv 1,4 \bmod 5$ و $s^2\equiv 1,4 \bmod 5$. إذا كان $r^2\equiv s^2 \bmod 5$ فإن $x\equiv 0 \bmod 5$، أي أن $5|x$. وإذا كان $r^2\not\equiv s^2 \bmod 5$ فإن $z\equiv 0 \bmod 5$، أي أن $5|z$.

مثال 59: جِد جميع الأعداد الصحيحة الموجبة n التي تجعل الثلاثي $(n,n+1,n+2)$ ثلاثي فيثاغورس بدائي.

الحل: أولاً الثلاثي المعطى يجب أن يُحقق معادلة فيثاغورس:

$$n^2+(n+1)^2=(n+2)^2$$

بالتبسط نحصل على المعادلة $n^2-2n-3=0$ أو $(n-3)(n+1)=0$ ومنه $n=3$ لأن $n>0$. هذه القيمة تعطينا الثلاثي $(3,4,5)$ وهو الثلاثي البدائي الوحيد الذي يُحقق شرط السؤال.

المعادلات الديوفانتية (Diophantine Equations)

نُطلِق على معادلة جبرية في متغيرين أو أكثر **معادلة ديوفانتية** إذا كان المطلوب هو إيجاد الأعداد الصحيحة التي تُحقق هذه المعادلة. أي زوج مرتب (x,y) (أو ثلاثي مرتب أو رباعي مرتب،...) مُكوَّن من أعداد صحيحة يُحقق المعادلة الديوفانتية يُسمى **حلاً صحيحاً** للمعادلة الديوفانتية.

فيما يأتي ذكرٌ لبعض الطرق الأساسية لحل المعادلات الديوفانتية:

1. استخدام الخواص العامة للأعداد الصحيحة.
2. استخدام التحليل.
3. استعمال التطابقات.
4. استخدام المتباينات.
5. استخدام خواص الرواسب التربيعية.

الأمثلة الآتية توضح هذه الطرق.

مثال 60: جِد الحلول الصحيحة للمعادلة $2x^2-6y^3+10z^4=45$.

الحل: لا يوجد أي حل للمعادلة لأن الطرف الأيسر دائماً عدد زوجي، بينما الطرف الأيمن عدد فردي.

مثال 61: جِد الحلول الصحيحة للمعادلة $x^3y-2x^2y^2z+xy^3z-1=0$.

الحل: من المعادلة نستنتج أن $xy \mid 1$ ومن ثم يصبح لدينا الحالات الآتية:

$$(x,y)=(1,1),\ (1,-1),\ (-1,1),\ (-1,-1)$$

بتعويض قيمة x و y لكل من هذه الحالات في المعادلة الأصلية نحصل على قيمة z المقابلة. الحلول هي

$$(x,y,z)=(1,1,0),\ (-1,-1,0)$$

مثال 62: جِد الحلول الصحيحة للمعادلة $x^3-8y^3=19$.

الحل: بالتحليل نحصل على المعادلة:

$$(x-2y)(x^2+2xy+4y^2)=19$$

هذا يؤدي إلى الاحتمالات الآتية:

$$\begin{cases} x-2y=\pm 1,\ \pm 19 \\ x^2+2xy+4y^2=\pm 19,\ \pm 1 \end{cases}$$

بحل هذه الأنظمة الأربعة نجد أن واحداً منها فقط يعطينا حلاً صحيحاً هو $(x,y)=(3,1)$.

مثال 63: جِد الحلول الصحيحة للمعادلة $9x^5-5y^2=14$.

الحل: إذا كانت توجد حلول صحيحة للمعادلة $9x^5-5y^2=14$ فإنه توجد حلول للتطابق $9x^5-5y^2\equiv 14 \bmod 3$، أو بالتبسيط، $y^2\equiv 2 \bmod 3$، وهذا مستحيل لأن $a^2\equiv 0,1 \bmod 3$ لأي عدد صحيح a. إذاً لا توجد حلول صحيحة للمعادلة المعطاة.

مثال 64: جِد الحلول الصحيحة للمعادلة $x^3-3y=50$.

الحل: بحساب المعادلة المعطاة قياس 3 نحصل على التطابق $x^3\equiv 2 \bmod 3$ الذي له حل وحيد هو $x\equiv 2 \bmod 3$. بكتابة

$x=2+3t$ و بالتعويض في المعادلة $x^3-3y=50$ نجد أن $y=9t^3+18t^2+8t-14$. إذاً يوجد للمعادلة عدد غير منتهٍ من الحلول الصحيحة معطاة كما يأتي:

$$(x,y)=(2+3t,9t^3+18t^2+8t-14)$$

حيث t عدد صحيح.

مثال 65: جِد الحلول الصحيحة للمعادلة $9x^6+5y^2=14$.

الحل: لاحظ أن $14=9x^6+5y^2\geq 5y^2$، أي أن $y^2\leq 14/5$. بما أن y عدد صحيح، إذاً $y^2=0$ أو $y^2=1$. إذا كان $y^2=0$، فبالتعويض في المعادلة المعطاة ينتج $9x^6=14$، وهي غير قابلة للحل. وإذا كان $y^2=1$، فبالتعويض في المعادلة المعطاة ينتج $x^6=1$ ومن ثم $x=\pm 1$. إذاً الحلول هي $(x,y)=(1,1),\ (1,-1),\ (-1,1),\ (-1,-1)$.

مثال 66: ما هي الحلول الصحيحة للمعادلة $y^2=x^3-x$.

الحل: نكتب المعادلة على الشكل الآتي:

$$y^2=x(x^2-1)$$

بملاحظة أن $(x,x^2-1)=1$، نستنتج من ذلك أن

$$\begin{cases} x=\pm a^2 \\ x^2-1=\pm b^2 \end{cases}$$

حيث a و b عددان صحيحان. بتعويض المعادلة الأولى في المعادلة الثانية نحصل على المعادلتين $a^4-1=\pm b^2$. في حالة $a^4-1=b^2$، $(x=a^2)$، أو $(a^2)^2-b^2=1$، فإنه بالتحليل يصبح لدينا $(a^2-b)(a^2+b)=1$ ومن ثم

$$\begin{cases} a^2-b=\pm 1 \\ a^2+b=\pm 1 \end{cases}$$

هذا يعطينا الحل $(a^2,b)=(1,0)$. هذا يقتضي أن $x=a^2=1$.

وفي حالة $a^4-1=-b^2$، $(x=-a^2)$، نحصل على $a^4+b^2=1$ التي حلولها هي $(a,b)=(\pm1,0), (0,\pm1)$. هذا يقتضي على التوالي $x=-a^2=-1$ و $x=-a^2=0$. إذاً حلول المعادلة الأصلية هي $(x,y)=(-1,0), (0,0), (1,0)$.

مثال 67: ما هي الحلول الصحيحة الموجبة للمعادلة $\frac{1}{x}+\frac{1}{y}+\frac{1}{z}=1$.

الحل: نفرض أولاً أن $x\le y\le z$ (لأن إعادة ترتيب المتغيرات x و y و z لن يغير من جوهر المعادلة). إذا كان $x=1$ فإن المعادلة تصبح $\frac{1}{y}+\frac{1}{z}=0$، وهذا مستحيل. إذا كان $x\ge4$ فسوف نحصل على $1=\frac{1}{x}+\frac{1}{y}+\frac{1}{z}\le\frac{1}{4}+\frac{1}{4}+\frac{1}{4}=\frac{3}{4}$، وهذا أيضاً مستحيل. إذاً لابد أن يكون $x=2$ أو $x=3$.

الحالة الأولى: $x=2$. في هذه الحالة تصبح المعادلة $\frac{1}{y}+\frac{1}{z}=\frac{1}{2}$. بما أن $y\le z$، إذاً $\frac{1}{2}=\frac{1}{y}+\frac{1}{z}\le\frac{2}{y}$ ومن ثم $y\le4$. لكن $y\ge x=2$. إذاً $2\le y\le4$. باختبار هذه القيم الثلاث للمتغير y نجد أن $y=3$ تعطي $z=6$ و $y=4$ تعطي $z=4$ للمعادلة $\frac{1}{y}+\frac{1}{z}=\frac{1}{2}$. هذا يعطينا الحلول

$$(x,y,z)=(2,3,6),\ (2,4,4)$$

الحالة الثانية: $x=3$. في هذه الحالة تصبح المعادلة $\frac{1}{y}+\frac{1}{z}=\frac{2}{3}$. بما أن $y\le z$، إذاً $\frac{2}{3}=\frac{1}{y}+\frac{1}{z}\le\frac{2}{y}$ ومن ثم $y\le3$. لكن $y\ge x=3$. إذاً $y=3$. بالتعويض نحصل على القيمة $z=3$. هذا يعطينا الحل

$(x,y,z)=(3,3,3)$ للمعادلة الأصلية.

عند إزالة الشرط $x \le y \le z$ نحصل على الحلول العشرة الآتية للمعادلة المعطاة:

$$(x,y,z)=(3,3,3),(2,3,6),(2,6,3)(3,2,6),(3,6,2),$$
$$(6,2,3),(6,3,2),(2,4,4),(4,2,4),(4,4,2)$$

مثال 68: جِد جميع الحلول الصحيحة الموجبة للمعادلة $2^n - 3^m = 1$.

الحل: لنفرض أولاً أن $n \ge 3$. بحساب المعادلة قياس 8 نحصل على التطابق $3^m \equiv 7 \bmod 8$ وهو غير قابل للحل لأن $3^m \equiv 1, 5 \bmod 8$ لأي عدد صحيح موجب m. إذاً لا توجد حلول للمعادلة إذا كان $n \ge 3$. بدراسة القيم $n=1$ و $n=2$ نجد أن الحل الوحيد للمعادلة المعطاة هو $(n,m)=(2,1)$.

مثال 69: ليكن d عدداً صحيحاً يقبل القسمة على عدد أولي $p \equiv 3 \bmod 4$. أثبت أن المعادلة $x^2 - dy^2 = -1$ غير قابلة للحل.

الحل: لنفرض أن المعادلة المعطاة قابلة للحل. إذاً التطابق $x^2 \equiv -1 \bmod p$ قابل للحل (لاحظ أن $p|d$). هذا يقتضي أن $\left(\frac{-1}{p}\right)=1$ وهذا تناقض واضح لأن $p \equiv 3 \bmod 4$ (أنظر الملحوظة 1 للنظرية 29). من هذا التناقض نستنتج أن المعادلة المعطاة غير قابلة للحل.

مثال 70: جِد الحلول الصحيحة للمعادلة $y^2 = x^3 + 23$.

الحل: نقوم بإثبات عدم وجود أي حل صحيح للمعادلة. لنفرض أن (x_0, y_0) هو حل للمعادلة المعطاة.

إذا كان x_0 عدداً زوجياً فسوف نحصل على التطابق

$y_0^2 \equiv 3 \bmod 4$ ، وهذا مستحيل لأن $a^2 \equiv 0,1 \bmod 4$ لأي عدد صحيح a. إذاً لابُد أن يكون x_0 عدداً فردياً، أي أنه إما $x_0 \equiv 1 \bmod 4$ أو $x_0 \equiv 3 \bmod 4$.

إذا كان $x_0 \equiv 3 \bmod 4$ فسوف نحصل على التطابق $y_0^2 \equiv 3^3 + 23 \equiv 2 \bmod 4$ ، وهذا مستحيل.

إذا كان $x_0 \equiv 1 \bmod 4$ فنبدأ أولاً بكتابة المعادلة على الشكل الآتي:

$$y_0^2 + 4 = x_0^3 + 27 = (x_0 + 3)(x_0^2 - 3x_0 + 9)$$

حيث إن $x_0 \equiv 1 \bmod 4$ فإن $x_0^2 - 3x_0 + 9 \equiv 1 - 3 + 9 \equiv 3 \bmod 4$ ومن ثم فلابد أن يقبل القسمة على عدد أولي p يُحقق $p \equiv 3 \bmod 4$ (لأن ضرب أعداد مُطابقة لـ 1 قياس 4 ينتج عدداً مُطابقاً لـ 1 قياس 4). هذا يقتضي أن $y_0^2 + 4 \equiv 0 \bmod p$ أو $y_0^2 \equiv -4 \bmod p$. من ذلك نستنتج أن

$$1 = \left(\frac{y_0^2}{p}\right) = \left(\frac{-4}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{4}{p}\right) = (-1)(1) = -1$$

وهذا أيضاً مستحيل. إذاً لا يوجد أي حل صحيح للمعادلة المعطاة.