الفصل الثالث

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

الحلول

1. من فرض السؤال نستنتج وجود أعداد صحيحة x و y و z بحيث $a-1=rx$ و $b-1=ry$ و $c-1=rz$. هذا يقتضي أنَّ

$$\begin{aligned} abc-1 &= (rx+1)(ry+1)(rz+1)-1 \\ &= r^3xyz+r^2(xy+xz+yz)+r(x+y+z) \end{aligned}$$

نستنتج من ذلك أنَّ $r \mid abc-1$.

2. أي عدد n يمكن كتابته بإحدى الصيغ الآتية: $4l,\ 4l+1,\ 4l+2,\ 4l+3$.

إذا كان $n=4l$ فإن $4 \mid n(n^2+3)$. وإذا كان $n=4l+1$ فإن $n^2+3=16l^2+8l+4$ ومن ثم $4 \mid n(n^2+3)$. إذا كان $n=4l+3$ فإن $n^2+3=16l^2+24l+12$ ومن ثم $4 \mid n(n^2+3)$. لكن إذا كان $n=4l+2$ فإن $n^2+3=16l^2+16l+7$ عدد فردي، لذا فالعدد $n(n^2+3)$ يقبل القسمة على 2 ولا يقبل القسمة على 4. لذا $4 \mid n(n^2+3)$ إذا وفقط إذا كان $n \neq 4l+2$.

3. لاحظ أولاً أن أي عدد n يمكن أن يأخذ إحدى الصيغ الآتية: $5l,\ 5l+1,\ 5l+2,\ 5l+3,\ 5l+4$. إذا كان $5 \mid 3n-1$ فلابد أن تكون n على الصيغة $5l+2$. حيث إن $3n^3-n^2+3n-1=(3n-1)(n^2+1)$ و $5 \mid n^2+1$، إذاً $25 \mid 3n^3-n^2+3n-1$.

4. الإثبات ينتج مباشرة من العلاقة $5(3n+7m)-3(5n+6m)=17m$.

5. لاحظ أن $7^3+8^3 | (7^3)^{15}+(8^3)^{15}$ و $6^3+9^3 | (6^3)^{15}+(9^3)^{15}$. بما أن

$$6^3+9^3=(6+9)(36-54+81)=3^3\times5\times7$$
$$7^3+8^3=(7+8)(49-56+64)=5\times9\times17$$

إذاً $45 | 6^{45}+9^{45}$ و $45 | 7^{45}+8^{45}$ ومن ثم $45 | 6^{45}+7^{45}+8^{45}+9^{45}$.

6. باستخدام نظرية ذات الحدين نجد أن

$$7^n=(6+1)^n=\sum_{i=0}^{n}\binom{n}{i}6^i=1+6n+\sum_{i=2}^{n}\binom{n}{i}6^i$$

حيث إنَّ $36 | \sum_{i=2}^{n}\binom{n}{i}6^i$، إذاً $36 | 7^n-6n-1$.

7. لنضع $M=(n^3-1)n^3(n^3+1)$.

إذا كان n عدداً زوجياً فإن $n=2k$ ومن ثم $8 | n^3$. هذا يقتضي أن $8 | M$. إذا كان n عدداً فردياً فإنه إما $n=4k+1$ أو $n=4k+3$. في حالة $n=4k+1$ نجد بسهولة أن $2 | n^3+1$ و $4 | n^3-1$. وفي حالة $n=4k+3$ نجد بسهولة أن $4 | n^3+1$ و $2 | n^3-1$. في كلتا الحالتين نجد أن $8 | M$.

إذا كان $n=3k$ فإن $9 | n^3$. إذا كان $n=3k+1$ فإن $9 | n^3-1$ وإذا كان $n=3k+2$ فإن $9 | n^3+1$. إذاً في جميع الحالات $9 | M$.

إذا كان $n=7k$ فإن $7 | n^3$. إذا كان $n=7k+1, 7k+2, 7k+4$ فإن $7 | n^3-1$. وإذا كان $n=7k+3, 7k+5, 7k+6$ فإن $7 | n^3+1$. إذاً في جميع الحالات $7 | M$.

الآن بـمـا أن $(7,8,9)=1$، إذاً $7\times 8\times 9|M$، أي أن $504|(n^3-1)n^3(n^3+1)$.

8. لنكتب $a\alpha=m$ و $b\alpha=n$ حيث m و n عددان صحيحان. هـذا يقتضي أن $\alpha=\frac{m}{a}=\frac{n}{b}$ ومـن ثـم $an=bm$. بـما أن $a|bm$ و $(a,b)=1$، إذاً $a|m$. أيضاً بما أن $b|an$ و $(a,b)=1$ فـإن $b|n$. مـن كلتا الحالتين نستنتج أن $\alpha=\frac{m}{a}=\frac{n}{b}$ عدد صحيح.

9. بملاحظة أن $a<\frac{a+b}{2}<b<c$ نجد أن $a+b<2c$. حيث إنَّ $c|a+b$ و $a+b<2c$ نستنتج من ذلك أن $c=a+b$. هـذا بـدوره يقتضي أن $a+c=2a+b$. حيث إنَّ $b|a+c$، إذاً $b|2a$. هـذا يقتضي أن $b=2a$ لأن $2a<2b$. نستنتج مـن ذلـك أن $c=a+b=3a$. إذاً الأعداد المطلوبة هي $a=n$، $b=2n$، $c=3n$ حيث n عـدد صـحيح موجب.

10. لاحظ أولاً أن القسمة $19|n^3+2n^2+n+1$ متحققة عند القيمة $n=2$. إذاً بأخذ القيم $n=2+19k$، حيث k عدد صحيح، نلاحظ أيضاً أن $19|(2+19k)^3+2(2+19k)^2+(2+19k)+1$.

11. بتحليل المقدار $n^{n-1}-1$ نحصل على الآتي:

$$n^{n-1}-1=(n-1)(n^{n-2}+n^{n-3}+\cdots+n+1)$$

نقوم بكتابة الحد الثاني في الطرف الأيمن على الشكل الآتي:

$$
\begin{aligned}
n^{n-2}+n^{n-3}+\cdots+n+1 \\
&=(n^{n-2}-1)+(n^{n-3}-1)+\cdots+(n-1)+[1+(n-2)] \\
&=(n^{n-2}-1)+(n^{n-3}-1)+\cdots+(n-1)+(n-1)
\end{aligned}
$$

هذا يقتضي أن $n-1$ يقسم $n^{n-2}+n^{n-1}+\cdots+n+1$ ومن ثم نستنتج من المعادلة الأولى أن $(n-1)^2$ يقسم $n^{n-1}-1$.

12. نريد أن نثبت أن $\dfrac{(n+1)(n+2)(n+3)\cdots(2n)}{2^n}$ عدد صحيح. بضرب بسط الكسر و مقامه بالعدد $n!$ نحصل على

$$
\begin{aligned}
\frac{(n+1)(n+2)(n+3)\cdots(2n)}{2^n} &= \frac{(2n)!}{2^n\cdot n!} \\
&= \frac{(2n)!}{2\cdot 4\cdot 6\cdot\dots\cdot(2n)} \\
&= 1\cdot 3\cdot 5\cdot\dots\cdot(2n-1)
\end{aligned}
$$

وهو المطلوب.

13. من العلاقة

$$
\binom{2n}{n}=\frac{(2n)!}{n!n!}=\frac{n+1}{n}\cdot\frac{(2n)!}{(n-1)!(n+1)!}=\frac{n+1}{n}\binom{2n}{n-1}
$$

نستنتج أن

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

بما أن $n+1 \mid n\binom{2n}{n}$ و $(n+1,n)=1$، فإن $n+1 \mid \binom{2n}{n}$.

14. بملاحظة أن

$$\binom{kn}{n}=\frac{(kn)!}{n!\cdot(kn-n)!}=\frac{kn}{n}\cdot\frac{(kn-1)!}{(n-1)!\cdot(kn-n)!}=k\cdot\binom{kn-1}{n-1}$$

نستنتج أن $k \mid \binom{kn}{n}$.

15. حيث إنَّ $(a,b)=g$ فإنه بإمكاننا أن نكتب $a=ga_1$ و $b=gb_1$ حيث a_1 و b_1 عددان صحيحان. الآن المعادلة $g=ax+by$ تُصبح $1=a_1x+b_1y$. هذا يقتضي أن $(x,y) \mid 1$ ومن ثم $(x,y)=1$.

16. لِنفرض أن $\frac{a}{b}+\frac{c}{d}=\frac{ad+bc}{bd}$ عدداً صحيحاً، أي أن $bd \mid ad+bc$ هذا يقتضي أن $bd \mid b(ad+bc)=abd+b^2c$ ومن ثم $bd \mid b^2c$ ومنه $d \mid bc$. بما أن $(d,c)=1$ فإن $d \mid b$.

أيضاً $bd \mid d(ad+bc)=ad^2+bdc$ ومن ثم $bd \mid ad^2$ ومنه $b \mid ad$. بما أن $(a,b)=1$ فإن $b \mid d$. من $d \mid b$ و $b \mid d$ نستنتج أن $b=d$، وهذا يُناقِض مفروض السؤال. إذاً العدد $\frac{a}{b}+\frac{c}{d}$ ليس عدداً صحيحاً.

17. من المعطى $p^n \mid ab$ نستنتج أن $p \mid ab$. هذا يقتضي أنه إما $p \mid a$ أو $p \mid b$، لكن ليس كليهما لأن $p \nmid (a,b)$. إذاً يُمكننا أن نفرض أن $p \nmid a$. هذا يقتضي أن $(p,a)=1$ ومن ثم $(p^n,a)=1$ أيضاً. الآن بما أن $p^n \mid ab$ و $(p^n,a)=1$ فإننا نستنتج أن $p^n \mid b$.

18. بما أن $(a,b)=g$ فإنه يوجد عددان صحيحان x و y يحققان

$ax+by=g$. بضرب طرفي المعادلة في c نحصل على المعادلة

$$acx+bcy=gc$$

نلاحظ الآتي:

$$b\mid c \Rightarrow ab\mid ac \Rightarrow ab\mid acx$$
$$a\mid c \Rightarrow ab\mid cb \Rightarrow ab\mid bcy$$

هذا يقتضي أن $ab\mid acx+bcy$ وباستخدام المعادلة أعلاه نستنتج أن $ab\mid gc$.

19. لنفترض أن $k>1$. إذاً بأخذ $n=k$ نحصل على $(k,2k)=k\neq 1$، وهذا يناقض المعطى في السؤال. هذا بدوره يؤدي إلى أن $k=1$.

20. أي عدد صحيح n يأخذ إحدى الصيغ الآتية: $3k,\ 3k+1,\ 3k+2$.

* إذا كان $n=3k$ فإن $n^2+n+5=9k^2+3k+5$.
* إذا كان $n=3k+1$ فإن $n^2+n+5=9k^2+9k+7$.
* إذا كان $n=3k+2$ فإن $n^2+n+5=9k^2+15k+11$.

في جميع الحالات العدد 3 لا يقسم n^2+n+5. إذاً $(n^2+n+5,3)=1$.

21. ليكن $g=(n^2+n+1,n^3+n+1)$. لاحظ أولاً أن $(g,n)=1$: لو أن p عدد أولي يقسم g و n، فإن p يقسم 1 لأن g يقسم n^2+n+1. الآن بما أن $g\mid(n^3+n+1)-(n^2+n+1)=n^2(n-1)$ و $(g,n)=1$، إذاً

$g \mid n-1$. أيضـــاً $g \mid (n^3+n+1)-(n-1)(n^2+n+1)=n+2$.
هذا يقتضي أن $g \mid (n+2)-(n-1)=3$ ومن ثم $g=1$ أو $g=3$.

بما أن $g \mid n-1$ فإننا نستنتج أنه إذا كان $3 \nmid n-1$ فـإن $g=1$. أمـا إذا كان $3 \mid n-1$ فإن $3 \mid (n-1)+3=n+2$ أيضاً. لكن حيث إنَّ

$$n^2+n+1=(n^2-1)+(n+2)$$
$$n^3+n+1=(n^3-1)+(n+2)$$

فإننا نستنتج أن 3 يقسم n^2+n+1 و n^3+n+1، ومن ثم 3 يقسم g .
هذا يقتضي أنه إذا كان $3 \mid n-1$ فإن $g=3$.

22. لإثبات المطلوب يكفي أن نثبـت أن $(40n+13,28n+9)=1$.
باستخدام خوارزمية أقليدس نحصل على

$$40n+13=1(28n+9)+(12n+4)$$
$$28n+9=2(12n+4)+(4n+1)$$
$$12n+4=3(4n+1)+1$$
$$4n+1=(4n+1)1+0$$

هذا يقتضي أن $(40n+13,28n+9)=1$.

23. إذا كان $n=2$ فإن $(2(n!)+1,5(n!)+1)=(5,11)=1$. إذاً نفـرض أن $n \geq 3$. لنفـرض أن $(2(n!)+1,5(n!)+1)=d>1$. لـيكن p عدد أولي يقسم d . إذاً $p \mid 2(n!)+1$ و $p \mid 5(n!)+1$. هذا يقتضي أن p يقسـم الفـرق، أي $p \mid 3(n!)$ ومـن ثـم إمـا $p \mid 3$ أو $p \mid n!$. في كلتـا الحالتين لابد أن يكون $p \leq n$ (لأن $n \geq 3$). هذا يقتضي أن $p \mid 2(n!)$. لكن $p \mid 2(n!)+1$ أيضاً. إذاً $p \mid 1$ وهذا مسـتحيل. هـذا يعنـي أن $d=1$ ومن ثم $(2(n!)+1,5(n!)+1)=1$.

24. لنضع $g=(a+b,a-b,ab)$. حيث إنَّ $g \mid a+b$ و $g \mid a-b$ فإن $g \mid b(a+b)=ab+b^2$ و $g \mid a(a-b)=a^2-ab$. وبسبب أن $g \mid ab$ نستنتج أن $g \mid b^2$ و $g \mid a^2$. هذا يقتضي أن $g \mid (a^2,b^2)$. لكن $(a,b)=1$ يقتضي أن $(a^2,b^2)=1$. إذاً $g \mid 1$ ومن ثم $g=1$، أي أن $(a+b,a-b,ab)=1$.

25. لِنفرض أن $t \geq k$. إذاً $p^{k+1} \mid ap^k+bp^t=p^k(a+bp^{t-k})$ يقتضي أن $p \mid a+bp^{t-k}$. إذا كان $t-k \neq 0$ فإن هذا يقتضي أن $p \mid a$ وهذا مستحيل لأن $(p,a)=1$. إذاً لابد أن يكون $t-k=0$، أي أن $k=t$ ومن ثم $p^{k+1} \mid ap^k+bp^k$ أي أن $p \mid a+b$.

26. إذا كان $a=b$ فإن المساواة $(a,b)=[a,b]$ متحققة. نُثبت الآن العكس. يُمكننا أن نكتب تحليل العددين a و b إلى عواملهما الأولية على الصورة $a=\prod_{i=1}^{r} p_i^{\alpha_i}$ و $b=\prod_{i=1}^{r} p_i^{\beta_i}$ حيث $\alpha_i \geq 0$ و $\beta_i \geq 0$ لجميع القيم $1 \leq i \leq r$. في هذه الحالة يصبح لدينا

$$(a,b)=\prod_{i=1}^{r} p_i^{\min(\alpha_i,\beta_i)}, \quad [a,b]=\prod_{i=1}^{r} p_i^{\max(\alpha_i,\beta_i)}$$

حيث $\min(\alpha_i,\beta_i)$ يساوي العدد الأصغر بين العددين α_i و β_i، و $\max(\alpha_i,\beta_i)$ يساوي العدد الأكبر بين العددين α_i و β_i. إذا كان $(a,b)=[a,b]$، فإنه لجميع القيم $1 \leq i \leq r$ يصبح لدينا $\min(\alpha_i,\beta_i)=\max(\alpha_i,\beta_i)$، أي $\alpha_i=\beta_i$. هذا يقتضي أن $a=b$. إذاً $(a,b)=[a,b]$ إذا وفقط إذا كان $a=b$.

27. لِنضع $g=(a,b)$. إذاً $a=gr_1$ و $b=gr_2$ حيث r_1 و r_2

عددان صحيحان موجبان يُحقِقان $(r_1,r_2)=1$. لاحظ أيضاً أن

$$a+b=g(r_1+r_2)$$
$$[a,b]=[gr_1,gr_2]=g[r_1,r_2]=gr_1r_2$$

لأن $(r_1,r_2)=1$ و $(r_1,r_2)[r_1,r_2]=r_1r_2$ يقتضي أن $[r_1,r_2]=r_1r_2$. بما أن

$$(a+b,[a,b])=(g(r_1+r_2),gr_1r_2)=g(r_1+r_2,r_1r_2)$$

فإن الإثبات سوف يتم إذا أثبتنا أن $(r_1+r_2,r_1r_2)=1$. لِنضع $(r_1+r_2,r_1r_2)=h$. بما أن $h\mid r_1+r_2$ و $h\mid r_1r_2$ فإن

$$h\mid r_1(r_1+r_2)-r_1r_2\Rightarrow h\mid r_1^2$$
$$h\mid r_2(r_1+r_2)-r_1r_2\Rightarrow h\mid r_2^2$$

ومن ثم $h\mid(r_1^2,r_2^2)$. لكن $(r_1,r_2)=1$ يقتضي أن $(r_1^2,r_2^2)=1$. إذاً $h\mid 1$ ومن ثم $h=1$ وبهذا يتم الإثبات.

28. لإثبات المساواة

$$([a,b],[a,c],[b,c])=[(a,b),(a,c),(b,c)]$$

نقوم بإثبات أن العدد الأولي p مرفوع لنفس الأُس في كلا الطرفين. لتكن الأعداد α و β و γ هي أُسس العدد p الموجودة للأعداد a و b و c على التوالي. بما أن ترتيب الأعداد a و b و c في المساواة أعلاه لن يغير من جوهر المساواة، فإنه بإمكاننا أن نفرض أن

$$\alpha\geq\beta\geq\gamma\geq 0$$

هذا يقتضي أن $[a,b]$ و $[a,c]$ و $[b,c]$ تحتوي العدد p مرفوعاً للأُسس α و α و β على التوالي. أذاً $([a,b],[a,c],[b,c])$ يحتوي العدد p مرفوعاً للأُس β.

أيضاً الأعداد (a,b) و (a,c) و (b,c) تحتوي العدد p مرفوعاً للأُسس β و β و γ على التوالي. إذاً $[(a,b),(a,c),(b,c)]$ يحتوي العدد p مرفوعاً للأُس β.

إذاً كلا الطرفين يحتوي على العدد الأولي p مرفوعاً لنفس الأُس. هذا يقتضي تساوي الطرفين.

29. حيث إنَّ $(x,y)=7$، فإنه يوجد عددان صحيحان موجبان x_0 و y_0 بحيث $x=7x_0$ و $y=7y_0$. بالتعويض في المعادلة $x+8y=245$ نحصل على المعادلة $x_0+8y_0=35$ والتي حلولها الموجبة هي $(x_0,y_0)=(27,1),\ (19,2),\ (11,3),\ (3,4)$. هذا يقتضي أن الحلول المطلوبة هي

$$(x,y)=(198,7),\ (133,14),\ (77,21),\ (21,28)$$

30. لِنضع $g=(2^m-1,2^n+1)$. هذا يقتضي وجود عددين صحيحين k و l حيث $2^m-1=kg$ و $2^n+1=\lg$، أي أن $2^m=kg+1$ و $2^n=\lg-1$. من ذلك نستنتج أن

$$2^{mn}=(kg+1)^n=sg+1,$$
$$2^{mn}=(\lg-1)^m=tg-1$$

حيث s و t عددان صحيحان (في المعادلة الثانية استخدمنا المعلومة m عدد فردي). بطرح المعادلتين السابقتين نحصل على المعادلة $g(t-s)=2$. هذا يقتضي أن $g\mid 2$ ومن ثم $g=1$ لأن كلا العددين 2^m-1 و 2^n+1 فردي. إذاً $(2^m-1,2^n+1)=1$.

31. نضع $T_n=\dfrac{a^n-b^n}{a-b}$ و نبدأ الحل بالملاحظة الآتية:

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

بالقسمة على $a-b$ نحصل على

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

أو بشكل مُختَصَر

$$T_n=(a-b)L+nb^{n-1}..........(*)$$

حيث L عدد صحيح. الآن نضع $g_1=(T_n,a-b)$ و $g_2=(a-b,n)$.

ليكن $d=(g_1,b)$. أذاً $d\,|\,g_1$ و $d\,|\,b$. بما أن $g_1\,|\,a-b$ إذاً $d\,|\,a-b$. هذا يقتضي أن $d\,|\,(a-b)+b$ أو $d\,|\,a$ ومن ثم $d\,|\,(a,b)=1$ ومنه $d=1$، أي أن $(g_1,b)=1$.

بما أن $g_1\,|\,T_n$ و $g_1\,|\,a-b$ فإنه من العلاقة (*) نستنتج أن $g_1\,|\,nb^{n-1}$. هذا يقتضي أن $g_1\,|\,n$ لأن $(g_1,b)=1$. بملاحظة أن $g_1\,|\,a-b$ و $g_1\,|\,n$ نستنتج أن $g_1\,|\,(a-b,n)$، أي أن $g_1\,|\,g_2$.

أيضاً بما أن $g_2\,|\,a-b$ و $g_2\,|\,n$ فإنه من العلاقة (*) نستنتج أن $g_2\,|\,T_n$. بملاحظة أن $g_2\,|\,T_n$ و $g_2\,|\,a-b$ نستنتج أن $g_2\,|\,(T_n,a-b)$، أي أن $g_2\,|\,g_1$.

الآن نستنتج من $g_1\,|\,g_2$، $g_2\,|\,g_1$، $g_1>0$، $g_2>0$ أن $g_1=g_2$

وهو المطلوب.

حلٌ آخر: نضع $t=a-b$. باستخدام العلاقة $(xy+z,x)=(z,x)$ نحصل على

$$\left(\frac{a^n-b^n}{a-b},a-b\right)=\left(a^{n-1}+a^{n-2}b+\cdots+b^{n-1},t\right)$$
$$=((t+b)^{n-1}+(t+b)^{n-2}b+\cdots+b^{n-1},t)$$
$$=(b^{n-1}+b^{n-2}b+\cdots+b^{n-1},t)$$
$$=(nb^{n-1},t)=(nb,t)$$
$$=(nb,a-b)=(n,a-b)$$

لأن $(b,a-b)=(a,b)=1$.

32. ليكن $a>1$ هو أصغر القواسم الموجبة للعدد n. إذا كان a عدداً مؤلفاً، فبإمكاننا كتابة $a=bc$، حيث إنَّ $1<b\le c<a$. هذا يقتضي أن العدد b هو عدد موجب أصغر من العدد a ويقسم العدد n. هذا التناقض يُثبِت أن العدد a عددٌ أولي.

33. حيث إنَّ $p+1$ عدد زوجي، فإن $p+1$ تأخذ إحدى الصور الآتية: $6k,\ 6k+2,\ 6k+4$. إذا كان $p+1=6k+2$، فإن $p+2=6k+3=3(2k+1)$ عدد غير أولي ($p>3$ يقتضي أن $k>0$). وإذا كان $p+1=6k+4$، فإن $p=6k+3=3(2k+1)$ عدد غير أولي ($p>3$ يقتضي أن $k>0$). هذا التناقض يقتضي أن $p+1=6k$ ومن ثم $6\mid p+1$.

34. لنكتب $pq+1=n^2$. إذاً $pq=(n-1)(n+1)$. لأن n عدد

زوجـــي، نجــد بســـهولة أن $(n-1,n+1)=1$. حيــث إنَّ $p<q$ و $n-1<n+1$ نستنتج أن $p=n-1$ و $q=n+1$ ومن ثم $q=p+2$.

35. نلاحـظ أولاً أن $(m,n)=1$. لِنأخـذ عـدداً أوليـاً p_j حيـث $1\le j\le t$. إذا كـان $1\le j\le i$ فـإن $p_j \mid m$ و $p_j \nmid n$. هـذا يقتضيـ أن $p_j \nmid m+n$. و إذا كــان $i+1\le j\le t$ فــإن $p_j \mid n$ و $p_j \nmid m$. هــذا يقتضي أن $p_j \nmid m+n$. نستنتج من ذلـك أن $m+n$ غـير قابـل للقسـمة على أيٍّ من الأعداد الأولية $p_1,p_2,\cdots,p_t$.

الآن لو فرضنا أنه يوجد عدد منتهٍ من الأعداد الأولية $p_1,p_2,\cdots,p_t$ فإن المناقشة أعلاه تقتضي أن $m+n$ يقبل القسمة على عدد أولي p مُختلـف عن الأعداد الأولية $p_1,p_2,\cdots,p_t$، وهـذا تنـاقض. هـذا يعنـي أن فـرض وجود عدد منتهٍ من الأعداد الأولية غير صحيح ومن ثـم يوجـد عـدد غـير منتهٍ من الأعداد الأولية.

36. ليكن p هو أصـغر عـدد أولي يقسـم $n!+1$ حيـث $n>1$. إذا كان $p\le n$ فإن $p\mid n!$. هـذا يقتضيـ أن $p\mid (n!+1)-n!$، أي أن $p\mid 1$ وهذا تناقض. إذاً لابد أن يكون $p>n$.

الآن لِنأخذ أيَ عدد طبيعي $n>1$. باستخدام المناقشة أعلاه نسـتنتج وجود عدد أولي p يُحقِق $p>n$، أي أنه يوجد عدد أولي أكبر من أي عـدد طبيعي معطى. هذا يُثبِت وجود عدد غير منتهٍ من الأعداد الأولية.

37. لِنفرض وجود عدد منتهٍ من الأعـداد الأوليـة ذات الشـكل العـام $6n+5$، ولـــتكن $p_1=5,p_2=11,p_3,\cdots,p_r$. نُعـــرف العـــدد $N=6p_2p_3\cdots p_r+5$. بما أن N عدد صورته العامة هي $6n+5$ فلابُـد

أن يكون أحد عوامله الأولية له نفس الصورة العامة $6n+5$،(لو كانت الصورة العامة لجميع العوامل الأولية للعدد N هي $6n+1$ فإن الصورة العامة للعدد N ستكون $6n+1$، وهذا تناقض). لِنُسمي هذا العامل الأولي p_i، حيث i يُحقق $2 \le i \le r$. الآن بما أن $p_i \mid N$ و $p_i \mid 6p_2p_3\cdots p_r$ فإن $p_i \mid 5$، وهذا تناقض لأن $p_i > 5$. من هذا التناقض نستنتج وجود عدد غير منتهٍ من الأعداد الأولية ذات الشكل العام $6n+5$.

38. بملاحظة أن $19 = 27 - 8$، فإن العبارة المعطاة يمكن كتابتها بالصيغة الآتية:

$$\left(3^{2n+1}+3\right)^3 - 8 = \left(3^{2n+1}+1\right)\left(\left(3^{2n+1}+3\right)^2 + 2\left(3^{2n+1}+3\right)+4\right)$$

حيث إنَّ كلا الحدين في الطرف الأيمن أكبر من 1، إذاً العبارة المعطاة عدد مؤلف لجميع قيم $n \ge 1$.

39. نقوم بتحليل المقدار المعطى:

$$\begin{aligned} 4n^3+3n-7 &= 4n^3-4+3n-3 \\ &= 4(n-1)(n^2+n+1)+3(n-1) \\ &= (n-1)(4n^2+4n+7) \end{aligned}$$

إذا كان $n \ge 3$، فإن $n-1 \ne 1$ و $4n^2+4n+7 \ne 1$ ومن ثم فالمقدار $4n^3+3n-7$ عدد مُؤلَّف. باختبار القيمتين $n=1$ و $n=2$ نجد أن $4n^3+3n-7$ عدد أولي إذا كان $n=2$ فقط.

40. الإثبات ينتج من التحليل الآتي:

$$n^5+n-1 = (n^2-n+1)(n^3+n^2-1)$$

كلا الحدين في الطرف الأيمن لا يساوي 1 عندما $n>1$.

41. لاحظ أولاً أن $R_n=\underbrace{111\cdots11}_{n}=\frac{10^n-1}{9}$. إذا كان n عدداً مؤلفاً، فإن $n=ab$ حيث $1<a,b<n$. بالتحليل نحصل على

$$R_n=R_{ab}=\frac{10^{ab}-1}{9}=\frac{10^a-1}{9}\times((10^a)^{b-1}+(10^a)^{b-2}+\cdots+10^a+1)$$

بما أن $9|10^a-1$ و $a>1$ و $b>1$ فإن كلا الحدين في الطرف الأيمن أكبر من 1. نستنتج من ذلك أن R_n عدد مؤلف.

42. كما في إجابة السؤال السابق، نلاحظ أولاً أن $R_k=\frac{10^k-1}{9}$.
باستخدام مثال 6 نحصل على الآتي:

$$\begin{aligned}9(R_n,R_m)&=(9R_n,9R_m)=(10^n-1,10^m-1)\\&=10^{(n,m)}-1=9R_{(n,m)}\end{aligned}$$

بالقسمة على 9 نحصل على المطلوب.

43. نبدأ الحل بكتابة $n=4k+r$، حيث $r=0,1,2,3$. لاحظ الآن ما يأتي:

$$\begin{aligned}R_n=R_{4k+r}&=\underbrace{11\cdots1}_{4k}\underbrace{00\cdots0}_{r}+\underbrace{11\cdots1}_{r}\\&=\underbrace{11\cdots1}_{4k}\times10^r+\underbrace{11\cdots1}_{r}\\&=1111\times100010001\cdots10001\times10^r+\underbrace{11\cdots1}_{r}\end{aligned}$$

حيث إن العدد $100010001\cdots10001$ يحتوي على $k-1$ مجموعة من الأصفار. بملاحظة أن $1111=11\times101$ وأن 101 لا يقسم $\underbrace{11\cdots1}_{r}$

عندما يكون $r=1,2,3$ فإننا نستنتج أن $101 | R_n$ إذا و فقط إذا كان $r=0$، أي أن $101 | R_n$ إذا و فقط إذا كان $4 | n$.

ملحوظة عامة:

$$R_{nm} = \underbrace{11\cdots1}_{nm} = \underbrace{11\cdots1}_{n} \times 1\underbrace{00\cdots0}_{n-1}1\underbrace{00\cdots0}_{n-1}1\cdots1\underbrace{00\cdots0}_{n-1}1$$

حيث إن مجموعة الأصفار $\underbrace{00\cdots0}_{n-1}$ مُكررة $m-1$ مرة.

44. يمكننا أن نأخذ $N=(k+1)!\times t+2$ أو $N=[(k+1)!]^t+2$ حيث $t=1,2,3,\cdots$.

45. لِنفرض أنه يوجد عدد صحيح موجب N بحيث إنَّ $p_n > n^2$ لجميع القيم $n \geq N$. هذا يقتضي أن $\frac{1}{n^2} < \frac{1}{p_n}$ لجميع القيم $n \geq N$. بما أن المتسلسلة $\sum_{n=1}^{\infty}\frac{1}{n^2}$ تقاربية، نستنتج أن المتسلسلة $\sum_{n=1}^{\infty}\frac{1}{p_n}$ تقاربية أيضاً، وهذا غير صحيح. و بهذا التناقض يتم الإثبات.

46. أي عدد صحيح $n>0$ يُمكِن كتابته على إحدى الصُوَر الآتية: $5k, 5k+1, 5k+2, 5k+3, 5k+4$، حيث $k \geq 0$. إذا كان $n=5k+4$ فإن $n+6=5(k+2)$ ليس عدداً أولياً. وإذا كان $n=5k+3$ فإن $n+12=5(k+3)$ ليس عدداً أولياً. وإذا كان $n=5k+2$ فإن $n+18=5(k+4)$ ليس عدداً أولياً. وإذا كان $n=5k+1$ فإن $n+24=5(k+5)$ ليس عدداً أولياً. أما إذا كان $n=5k$ فإن العدد الأولي الوحيد هو $n=5$ عندما يكون $k=1$. إذا كان $k>1$ فإن $n=5k$ ليس عدداً أولياً. بالتعويض نجد أنه عندما تكون

$n=5$ فإن جميع الأعـداد $5,5+6,5+12,5+18,5+24$ أعـداد أوليـة. نستنتج من ذلك أن العدد الوحيد الذي يُحقِق شرط السؤال هو $n=5$.

47. نريد أن نجِد عدداً صحيحاً موجباً x يحقق $p^n+1=x^2$

نـــدرس حـــالتين. عنـــدما $p=2$ نكتـــب المعادلـــة عـــلى الشـــكل $2^n=(x-1)(x+1)$. حيث إنَّ x عدد فردي، فإن $(x-1,x+1)=2$. هـــذا يقتـــضي أنـــه إمـــا $x-1=2$ و $x+1=2^{n-1}$ أو $x-1=2^{n-1}$ و $x+1=2$. في الحالة الأولى نحصل على $(p,n,x)=(2,3,3)$ وفي الحالـة الثانية لا يوجد أي حل.

عنـدما يكـون $p>2$ عـدداً أوليـاً فرديـاً فالمعادلـة تأخـذ الشـكل $p^n=(x-1)(x+1)$. حيث إنَّ x عدد زوجي، فإن $(x-1,x+1)=1$. هـــذا يقتضيـــ أنـــه إمـــا $x-1=1$ و $x+1=p^n$ أو $x-1=p^n$ و $x+1=1$. في الحالة الأولى نحصل عـلى $(p,n,x)=(3,1,2)$ وفي الحالـة الثانية لا يوجد أي حل.

إذاً p^n+1 مربع كامل عندما $(p,n)=(2,3),\ (3,1)$ فقط.

48. ليكن p عدداً أولياً يُحقق شرط السؤال. إذاً توجد أعـداد أوليـة $p_2>p_1$ و $q_2>q_1$ تُحقق

$$p=p_1+p_2,\quad p=q_2-q_1$$

بما أن $p_1+p_2>2$، فإن p عدد فردي. هذا يقتضيـ أنـه إمـا p_1 أو p_2 عدد زوجي وأنه إما q_1 أو q_2 عدد زوجـي. لـذا يُمكننـا أن نفـرض أن $p_1=q_1=2$ ومن ثم يُصبح لدينا الآتي:

$$p=2+p_2,\quad p=q_2-2$$

نستنتج من ذلك أن الأعداد الثلاثة $p-2, p, p+2$ أعداد أولية. وهذا ممكن فقط إذا كان $p=5$ (الإثبات متروك للقارئ). إذاً العدد الأولي $p=5$ هو العدد الأولي الوحيد الذي يمكن كتابته كفرق و كمجموع عددين أوليين آخرين.

49. من خواص الأعداد الزوجية و الفردية نستنتج أنه واحد فقط من الأعداد p ، q، r يجب أن يكون زوجياً. إذا كان $r=2$ فإن

$$2^3=(p+q)(p^2-pq+q^2)$$

وهذا مستحيل لأن p^2-pq+q^2 عدد فردي و $p^2-pq+q^2=(p-q)^2+pq>1$. أما إذا كان $p=2$ فإن

$$2^3=(r-q)(r^2+rq+q^2)$$

وهذا أيضاً مستحيل لأن r^2+rq+q^2 عدد فردي و $r^2+rq+q^2>1$. نحصل على نفس الاستنتاج إذا كان $q=2$. إذاً لا توجد أعداد أولية تُحقِق المعادلة $p^3+q^3=r^3$.

50. لنفرض أن المجموع المعطى عدد صحيح S:

$$S=1+\frac{1}{2}+\frac{1}{3}+\cdots+\frac{1}{n}$$

ليكن k أكبر عدد صحيح يحقق $2^k \le n$ (بما أن $n>1$ فإن $k\ge 1$). ضع $P=1\cdot 3\cdot 5\cdot\cdots\cdot(2r+1)$، حيث $2r+1\le n$. (أي أن P يساوي حاصل ضرب الأعداد الفردية التي هي أقل من أو تساوي n.) إذا كان S عدداً صحيحاً، فإن $2^{k-1}\cdot P\cdot S$ عدد صحيح أيضاً. لكن في المجموع $2^{k-1}\cdot P\cdot S$، جميع الحدود أعداد صحيحة ما عدا الحد $\frac{2^{k-1}\cdot P}{2^k}$، وهذا

تناقض واضح. إذاً نستنتج من ذلك أن S عدد غير صحيح.

51. لنفرض أن المجموع المعطى عدد صحيح S:

$$S = 1 + \frac{1}{3} + \frac{1}{5} + \cdots + \frac{1}{2n-1}$$

ليكن k أكبر عدد صحيح يحقق $3^k \le 2n-1$ (بما أن $n > 1$ فإن $k \ge 1$). ضع $P = 1\cdot 3\cdot 5\cdot \cdots \cdot (2n-1)$ (أي أن P يساوي حاصل ضرب الأعداد الفردية التي هي أقل من أو تساوي $2n-1$.) إذا كان S عدداً صحيحاً، فإن $3^{k-2}\cdot P\cdot S$ عدد صحيح أيضاً. لكن في المجموع $3^{k-2}\cdot P\cdot S$، جميع الحدود أعداد صحيحة ما عدا الحد $\frac{3^{k-2}\cdot P}{3^k}$، وهذا تناقض واضح. إذاً نستنتج من ذلك أن S عدد غير صحيح.

52. لنفرض أن $(n!)^2 + k = p^r$، حيث إنَّ p عدد أولي و $r \ge 1$. بما أن $2 \le k \le n$، إذاً $k \mid n!$. هذا يعني أن $k \mid (n!)^2 + k = p^r$ ومن ثم $k = p^t$ حيث $1 \le t \le r$. نلاحظ أيضاً أن $t \ne r$ وإلا سنحصل على $(n!)^2 + p^r = p^r$ أو $(n!)^2 = 0$، وهذا تناقض واضح. هذا يقتضي أن $1 \le t < r$. حيث إنَّ $(n!)^2 = p^r - k = p^t(p^{r-t}-1)$ و $k = p^t \mid n!$، إذاً $p^{2t} \mid p^t(p^{r-t}-1)$. بالتبسيط نحصل على $p^t \mid p^{r-t}-1$، وهذا تناقض واضح لأن $r \ne t$ و $t \ge 1$. بسبب هذا التناقض يكمل الإثبات.

53. لِنفرض أنه يوجد عدد طبيعي n_0 بحيث إنَّ $a_{n_0} = 5$. من الواضح إذاً أن $n_0 > 2$. هذا يقتضي أن أكبر العوامل الأولية للعدد $P_{n_0} = 1 + a_1 a_2 \cdots a_{n_0-1}$ يساوي 5، أي أن

$$P_{n_0} = 2^{\alpha} \times 3^{\beta} \times 5^{\gamma}, \quad \alpha \ge 0, \beta \ge 0, \gamma \ge 1.$$

بما أن P_{n_0} عدد فردي (لأن $a_1 = 2$) فإن $\alpha = 0$. أيضاً بما أن P_{n_0} عدد لا يقبل القسمة على 3 (لأن $a_2 = 3$) فإن $\beta = 0$. نستنتج من ذلك أن

$$P_{n_0} = 5^{\gamma}, \quad \gamma \geq 1$$

هذا يُعطينا

$$a_1 a_2 \cdots a_{n_0 - 1} = 5^{\gamma} - 1 = (5-1)(5^{\gamma-1} + \cdots + 5 + 1)$$

أو $(a_1 = 2)$

$$a_2 \cdots a_{n_0 - 1} = 5^{\gamma} - 1 = 2(5^{\gamma-1} + \cdots + 5 + 1)$$

أي أن $a_2 \cdots a_{n_0-1}$ عدد زوجي وهذا مستحيل لأن $a_i \neq 2$ لجميع القيم $i \geq 2$ (وذلك بسبب أن P_i عدد فردي لجميع القيم $i \geq 2$) لذا نستنتج أن $a_n \neq 5$ لجميع القيم $n \geq 1$.

54. لنفرض أن $\sqrt{n}$ عدد نسبي، أي أن

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

حيث a و $b \neq 0$ عددان صحيحان. نفرض أيضاً أن $(a,b) = 1$. بتربيع الطرفين نحصل على المساواة $a^2 = nb^2$. بما أن n ليس مربعاً كاملاً فإنه يوجد عدد أولي p وعدد صحيح $k \geq 0$ بحيث إنَّ $p^{2k+1} \parallel n$. من المساواة $a^2 = nb^2$ نستنتج أن $p \mid a^2$ ومن ثم $p \mid a$. لنكتب $a = p^r t$ حيث $r \geq 1$ و $(p,t) = 1$. حيث إنَّ $(a,b) = 1$ فإن $p \nmid b$. إذاً من المساواة $a^2 = nb^2$ نستنتج أن $p^{2r} \parallel a^2$ و $p^{2k+1} \parallel nb^2$، وهذا يناقض النظرية الأساسية للحساب (المساواة $a^2 = nb^2$ تُحتِم على العدد الأولي p أن يكون مرفوعاً لنفس القوة في كلا الطرفين). هذا التناقض يقتضي أن $\sqrt{n}$ عدد غير نسبي.

55. إذا كان $\log_b a$ عدداً نسبياً، فإنه يوجد عددان صحيحان

موجبان m و n بحيث $\log_b a = m/n$. هـذا يقتـضي أن $a = b^{m/n}$ أو $a^n = b^m$. بما أن $a > 1$ فإنه يوجد عدد أولي p يقسم a. هـذا يقتضي أن $p \mid b^m$ ومن ثم $p \mid b$. وهذا تناقض لأن $(a,b)=1$. من ذلك نستنتج أن $\log_b a$ عدد غير نسبي.

56. نفرض أن $\sin 1$ عدد غير نسبي و لنكتب $\sin 1 = \frac{m}{n}$ حيث m و $n \neq 0$ عددان صحيحان. نستخدم المتسلسلة $\sin 1 = \sum_{k=0}^{+\infty} \frac{(-1)^k}{(2k+1)!}$.
ليكن $2l+1$ أصغر عدد صحيح فردي موجب أكبر من أو يساوي n.
بضرب المتسلسلة السابقة بـ $(2l+1)!$ نحصل على الآتي:

$$(2l+1)!\frac{m}{n} = A_l + B_l$$

حيث

$$A_l = (2l+1)!\sum_{k=0}^{l} \frac{(-1)^k}{(2k+1)!}$$

$$\begin{aligned} B_l &= (2l+1)!\sum_{k=l+1}^{+\infty} \frac{(-1)^k}{(2k+1)!} \\ &= \pm\frac{1}{(2l+2)(2l+3)} \mp \frac{1}{(2l+2)(2l+3)(2l+4)(2l+5)} \pm \cdots \\ &= \pm a_1 \mp a_2 \pm \cdots \end{aligned}$$

بما أن $(2l+1)!\frac{m}{n}$ و A_l عددان صحيحان، فلابد أن يكون B_l عدداً صحيحاً أيضاً، وهذا مستحيل لأنه إما

$$0 < a_1 - a_2 < B_l < a_1 < 1$$

أو

$$-1 < -a_1 < B_l < -a_1 + a_2 < 0$$

أي أن B_i ليس عدداً صحيحاً. هذا التناقض يثبت أن $\sin 1$ عدد غير نسبي.

57. حيث إنَّ $(n,n+k)\,|\,k$، فإن المعادلة $nx+(n+k)y=k$ قابلة للحل. بملاحظة أن $x_0=-1$ و $y_0=1$ يحققان المعادلة، إذاً جميع الحلول معطاة على النحو الآتي:

$$x=-1+(n+k)t\,,\ y=1-nt$$

حيث t عدد صحيح.

58. نُكوِن المعادلة $\frac{x}{35}+\frac{y}{91}=\frac{1}{65}$، ومنها نحصل على المعادلة الخطية $91x+35y=49$ أو $13x+5y=7$. باستخدام خوارزمية القسمة نجد أن $x=14, y=-35$ هو أحد الحلول.(الحلول الأخرى هي $x=14+5t\,, y=-35-13t$ لأي عدد صحيح t) إذاً الكسران $\frac{14}{35}$ و $\frac{-35}{91}$ يحققان المطلوب.

59. بما أن $(153,119)=17$، فإنَّ المعادلة الخطية المعطاة قابلة للحل إذا كان $17\,|\,1000+m$. بملاحظة أن $1000=17(58)+14$، نجد أن أصغر عدد صحيح موجب m يحقق المطلوب هو $m=3$. بهذا العدد m، المعادلة تصبح $9x+7y=59$. الحل العام لهذه المعادلة هو (t عدد صحيح)

$$x=236+7t$$
$$y=-295-9t$$

60. بما أن $(a,b)=1\,|\,k$ فإن المعادلة $ax+by=k$ قابلة للحل.

ليكن (x_0, y_0) حلاً للمعادلة. إذاً جميع الحلول مُعطاة على النحو الآتي:

$$x = x_0 + bt, \ \ y = y_0 - at, \ \ t \in \mathbb{Z}$$

لكي يتحقق الشرطان $x \geq 0$ و $y \geq 0$ لابد أن نختار الأعداد الصحيحة t التي تُحقق الشرطين الآتيين

$$x_0 + bt \geq 0, \ \ y_0 - at \geq 0$$

هذا يقتضي أن t لابد أن تُحقق

$$\frac{-x_0}{b} \leq t \leq \frac{y_0}{a}$$

نستنتج من ذلك أنه إذا كان $b \mid x_0$ فإن عدد الحلول يساوي $\left[\!\left[\frac{y_0}{a} \right]\!\right] - \left[\!\left[\frac{-x_0}{b} \right]\!\right] + 1$، وإذا كان $b \nmid x_0$ فإن عدد الحلول يساوي $\left[\!\left[\frac{y_0}{a} \right]\!\right] - \left[\!\left[\frac{-x_0}{b} \right]\!\right]$.

61. حيث إنَّ $(5,22,18) = 1$ يقسم 3، فإنَّ المعادلة

$$5x + 22y + 18z = 3$$

قابلة للحل. نبدأ بكتابة x (لاحتوائه على أصغر معامل) بدلالة المتغيرين الآخرين

$$x = \frac{3 - 22y - 18z}{5} = -4y - 3z + \frac{3 - 2y - 3z}{5}$$

بما أن x عدد صحيح، إذاً لابد أن يكون $\frac{3 - 2y - 3z}{5}$ عدد صحيح، لنقل أنه t:

$$t = \frac{3 - 2y - 3z}{5}$$

نكتب الآن y (أيضاً لاحتوائه على أصغر معامل عند تجاهل الإشارة) بدلالة المتغيرين الآخرين

$$y=\frac{3-5t-3z}{2}=1-2t-z+\frac{1-t-z}{2}$$

حيث إنَّ y عدد صحيح، إذاً لابد أن يكون $\frac{1-t-z}{2}$ عدد صحيح، لنقل أنه u:

$$u=\frac{1-t-z}{2}$$

هذا يقتضي أن

$$z=1-t-2u$$
$$y=-t+3u$$
$$x=-3+8t-6u$$

حيث t و u عددان صحيحان، وهي تُمثل حلول المعادلة الخطية المعطاة.

62. بما أن $(7,-9,10,-11)=1$ يقسم 23، إذاً المعادلة

$$7x-9y+10z-11w=23$$

قابلة للحل. باستخدام الطريقة المستخدمة في السؤال السابق نحصل على الحل الآتي:

$$x=2+4t+u-v$$
$$y=-1+2t+3u-2v$$
$$z=-t+2u$$
$$w=v$$

حيث t,u,v أعداد صحيحة.

63. بما أن المجموعة $\{c_i+d_jm_1:1\le i\le m_1,1\le j\le m_2\}$

تحتوي على m_1m_2 عدد فلإثبات أن المجموعة تُمثِل نظام رواسب تام قياس m_1m_2 يكفي أن نُثبِت أن أي عددين من هذه المجموعة غير متطابقين قياس m_1m_2. لِنفرض أن

$$c_i + d_j m_1 \equiv c_k + d_l m_1 \mod m_1m_2$$

هذا يقتضي أن $c_i + d_j m_1 \equiv c_k + d_l m_1 \mod m_1$ أو $c_i \equiv c_k \mod m_1$ ومن ثم $c_i = c_k$ لأن $c_1, c_2, \cdots, c_{m_1}$ تُمثِل نظام رواسب تام قياس m_1. هذا يُعطينا التطابق

$$d_j m_1 \equiv d_l m_1 \mod m_1m_2$$

والذي بدوره يُعطينا $d_j \equiv d_l \mod m_2$ ومن ثم $d_j = d_l$ لأن $d_1, d_2, \cdots, d_{m_2}$ تُمثِل نظام رواسب تام قياس m_2. نستنتج من ذلك أن $c_i + d_j m_1 = c_k + d_l m_1$، أي أن أي عددين مُختلفين من المجموعة المعطاة لا يمكن أن يكونا متطابقين قياس m_1m_2. إذاً المجموعة $\{c_i + d_j m_1 : 1 \le i \le m_1, 1 \le j \le m_2\}$ تُمثل نظام تام قياس m_1m_2.

64. إذا كان $n = 2$ فإن العددين $1\cdot 2,\ 2\cdot 3$ لا يُمثِلان نظام رواسب تام قياس 2 لأن $1\cdot 2 \equiv 2\cdot 3 \mod 2$. وإذا كان $n = 3$ فإن الأعداد $1\cdot 2,\ 2\cdot 3,\ 3\cdot 4$ لا تُمثِل نظام رواسب تام قياس 3 لأن $2\cdot 3 \equiv 3\cdot 4 \mod 3$. و في حالة $n \ge 4$ فأيضاً الأعداد $1\cdot 2, 2\cdot 3, 3\cdot 4, \cdots, (n-2)\cdot(n-1), (n-1)\cdot n, n\cdot(n+1)$ لا تُمثِل نظام رواسب تام قياس n لأن $(n-2)\cdot(n-1) \equiv n^2 - 3n + 2 \equiv 2 \equiv 1\cdot 2 \mod n$. نستنتج من ذلك أن الأعداد $1\cdot 2, 2\cdot 3, 3\cdot 4, \cdots, n\cdot(n+1)$ لا تُمثِل نظام رواسب تام قياس أي عدد صحيح $n \ge 2$.

65. لاحظ أولاً أن $(a^3,p)=1$ لجميع الأعداد $a=1,2,\cdots,p-1$. بما أن المجموعة $\{1^3,2^3,\cdots,(p-1)^3\}$ تحتوي على $p-1$ عدد فإنه لإثبات أن المجموعة تُمثِل نظام رواسب مُختزَل قياس p يكفي أن نُثبِت أن أي عددين في المجموعة غير متطابقين قياس p. لِنأخذ عددين a و b بحيث إنَّ $1\le a,b\le p-1$ و

$$a^3\equiv b^3 \mod p$$

حيث إنَّ $(3,p-1)=1$ فإنه يوجد معكوس ضربي k $(1\le k\le p-1)$ قياس $p-1$ للعدد 3، أي أن $3k\equiv 1 \mod p-1$، أو $3k=1+l(p-1)$ حيث $l>0$ عدد صحيح. هذا يقتضي أن

$$a^{3k}\equiv b^{3k} \mod p \Rightarrow a^{1+l(p-1)}\equiv b^{1+l(p-1)} \mod p$$
$$\Rightarrow a\equiv b \mod p$$

ومن ثم $a=b$ لأن الأعداد $1,2,\cdots,p-1$ تمثل نظام رواسب مختزل قياس p. هذا يثبت أن المجموعة $\{1^3,2^3,\cdots,(p-1)^3\}$ تمثل نظام رواسب مُختزَل قياس p.

عندما يكون $(3,p-1)\neq 1$ فالنتيجة يمكن أن لا تتحقق. على سبيل المثال عندما نأخذ $p=7$ فإن $(3,p-1)=(3,6)=3\neq 1$ و الأعداد $1^3,2^3,\cdots,6^3$ لا تُمثِل نظام رواسب مُختزَل قياس 7 لأن $1^3\equiv 2^3 \mod 7$.

66. بإجراء الحسابات الآتية

$$7^2\equiv 4 \mod 15 \Rightarrow 7^4\equiv 1 \mod 15 \Rightarrow 7^{2^n}\equiv 1 \mod 15$$
$$8^2\equiv 4 \mod 15 \Rightarrow 8^4\equiv 1 \mod 15 \Rightarrow 8^{2^n}\equiv 1 \mod 15$$
$$9^2\equiv 6 \mod 15 \Rightarrow 9^4\equiv 6 \mod 15 \Rightarrow 9^{2^n}\equiv 6 \mod 15$$

نستنتج أن

$$4\cdot 7^{2^n}+5\cdot 8^{2^n}+6\cdot 9^{2^n}\equiv 4+5+36\equiv 0 \bmod 15$$

أي أن $15 | 4\cdot 7^{2^n}+5\cdot 8^{2^n}+6\cdot 9^{2^n}$.

67. بملاحظة أن $25\equiv 4 \bmod 21$ و

$$\begin{aligned}4^{n+2}+5^{2n+1}&=16\times 4^n+5\times 25^n\equiv 16\times 4^n+5\times 4^n\\&=21\times 4^n\equiv 0 \bmod 21\end{aligned}$$

نستنتج أن $21 | 4^{n+2}+5^{2n+1}$.

68. بملاحظة أن $36\equiv 2 \bmod 34$ و $2^5\equiv -2 \bmod 34$ نحصل على

$$36^{50}\equiv 2^{50}=(2^5)^{10}\equiv(-2)^{10}=(2^5)^2\equiv(-2)^2=4 \bmod 34$$

وبملاحظة أن $37\equiv 3 \bmod 34$ و $3^5\equiv 5 \bmod 34$ و $5^3\equiv 13 \bmod 34$ نحصل على

$$37^{50}\equiv 3^{50}\equiv 5^{10}\equiv 5(13)^3\equiv -3(13)^2\equiv -5(13)\equiv 3 \bmod 34$$

هذا يقتضي أن $36^{50}+37^{50}\equiv 4+3\equiv 7 \bmod 34$ ومن ثم فإن باقي قسمة $36^{50}+37^{50}$ على 34 يساوي 7.

69. حيث إنَّ $a\equiv 0,\pm1,\pm2,\pm3,\pm4 \bmod 9$، فبتكعيب الطرفين وبالتبسيط، نحصل على $a^3\equiv 0,\pm1 \bmod 9$.

70. لنفرض أنَّ $9n+5=a^3+b^3+c^3$. بحساب المعادلة قياس 9 وباستخدام السؤال السابق، نحصل على الاحتمالات التالية $5\equiv 0,\pm1,\pm2,\pm3 \bmod 9$، والتي جميعها خاطئة. إذاً لا يمكن كتابة أي

عدد ذي الصيغة $9n+5$ كمجموع ثلاثة أعداد مكعبة.

71. الأعداد الزوجية تُحقق التطابق $x \equiv 0 \bmod 2$. الأعداد الفردية تُحقق التطابق $x \equiv 1, 3, 5, 7, 9, 11 \bmod 12$. إذا كان $x \equiv 3, 9 \bmod 12$، فإن $x \equiv 0 \bmod 3$. وإذا كان $x \equiv 1, 5 \bmod 12$، فإن $x \equiv 1 \bmod 4$. وإذا كان $x \equiv 7 \bmod 12$، فإن $x \equiv 1 \bmod 6$. الاحتمال الأخير $x \equiv 11 \bmod 12$ يبقى كما هو.

72. بإجراء الحسابات الآتية، نحصل على المطلوب:

$$3^5 = 27 \times 9 \equiv 10 \times 9 \equiv 5 \bmod 17$$
$$3^{15} \equiv 5^3 \equiv 8 \times 5 \equiv 6 \bmod 17$$
$$3^{30} \equiv 6^2 \equiv 2 \bmod 17$$

73. لاحظ أولاً أن $10^n \equiv 1 \bmod 3$. هذا يعني أنه يمكننا أن نكتب $10^n = 3k + 1$، حيث k عدد صحيح موجب. بالحسابات الآتية نحصل على المطلوب:

$$2^{10^n} = 2^{3k+1} = 8^k \times 2 \equiv 1^k \times 2 \equiv 2 \bmod 7$$

74. يمكننا استخدام الاستقراء الرياضي لإثبات المطلوب بسهولة. سوف نقوم باستخدام طريقة أُخرى. لاحظ أولاً أن $5^n \equiv 0 \bmod 25$ إذا كان $n \geq 2$. وحيث إنَّ $5 \equiv 1 \bmod 4$ فإن $5^n \equiv 1 \bmod 4$ لجميع القيم $n \geq 2$. هذا يعطينا النظام الآتي:

$$5^n \equiv 0 \bmod 25$$
$$5^n \equiv 1 \bmod 4$$

بوضع $x = 5^n$ ومن ثم حل النظام بواسطة نظرية الباقي الصينية، نجد أن الحل هو $x \equiv 25 \bmod 100$، أي أن $5^n \equiv 25 \bmod 100$.

75. نقوم بحساب العددين !11 و !21 قياس 23. نحصل أولاً على

$$\begin{aligned}
11! &= 11\times(10\times 9)\times(8\times 7)\times(6\times 5)\times(4\times 3\times 2\times 1)\\
&\equiv 11\times(-2)\times(10)\times(7)\times(1)\\
&= (-22)\times(70)\\
&\equiv (1)\times(1)\\
&\equiv 1 \bmod 23
\end{aligned}$$

أيضاً نلاحظ ما يأتي:

$$\begin{aligned}
21! &= 11!\times 12\times 13\times 14\times\cdots\times 20\times 21\\
&\equiv 11!\times(-11)\times(-10)\times(-9)\times\cdots\times(-3)\times(-2)\\
&\equiv 11!\times 11!\\
&\equiv 1\times 1\\
&\equiv 1 \bmod 23
\end{aligned}$$

هذا يقتضي أن $21! \equiv 11! \bmod 23$.

76. أي عدد أولي $p \geq 5$ يُحقق إحدى التطابقات الآتية $p \equiv 1, 5, 7, 11 \bmod 12$. بتربيع الطرفين نحصل على المطلوب:

$$\begin{aligned}
p^2 &\equiv 1,\ 25,\ 49,\ 121 \bmod 12\\
&\equiv 1,\ 1,\ 1,\ 1 \bmod 12\\
&\equiv 1 \bmod 12
\end{aligned}$$

77. أولاً لاحظ أن $p \geq 2$ يقتضي أن $p^2 + 2^p > 3$. إذا كان $p = 2$ فإن $p^2 + 2^p = 8$ عدد غير أولي. نفرض الآن أن p عدد أولي

فردي. إذا كان $p \equiv 1 \bmod 3$ فإن

$$p^2 + 2^p \equiv 1^2 + (-1)^p \equiv 0 \bmod 3$$

ومن ثم $p^2 + 2^p$ عدد غير أولي. إذا كان $p \equiv 2 \bmod 3$ فإن

$$p^2 + 2^p \equiv 2^2 + (-1)^p \equiv 0 \bmod 3$$

ومن ثم $p^2 + 2^p$ عدد غير أولي. إذا كان $p \equiv 0 \bmod 3$ فلابد أن يكون $p = 3$ لأن p عدد أولي. في هذه الحالة $p^2 + 2^p = 9 + 8 = 17$ عدد أولي. إذاً يوجد عدد أولي وحيد هو $p = 3$ يجعل $p^2 + 2^p$ عدداً أولياً.

78. لنكتب

$$\begin{aligned} N &= a_{2k+1}a_{2k}\cdots a_3a_2a_1a_0 \\ &= a_{2k+1}a_{2k} \times 100^k + \cdots + a_3a_2 \times 100 + a_1a_0 \end{aligned}$$

حيث $0 \le a_i \le 9$ لجميع القيم i. بما أن $100 \equiv 1 \bmod 99$، فإن

$$N \equiv a_{2k+1}a_{2k} + \cdots + a_3a_2 + a_1a_0 \bmod 99$$

أي أن N يقبل القسمة على 99 إذا وفقط إذا كان مجموع الأرقام المُكوِنة للعدد N مأخوذة مثنىً مثنى، ومبتدئاً من خانة الآحاد، يقبل القسمة على 99. فعلى سبيل المثال

$$546312 \equiv 54 + 63 + 12 = 129 \equiv 30 \bmod 99$$
$$396 \equiv 3 + 96 = 99 \equiv 0 \bmod 99$$

أي أن $99 \nmid 546312$ و $99 \mid 396$.

79. نُلاحِظ أولاً أن $1000 = 27 \times 37 + 1 \equiv 1 \bmod 27$. نأخذ عدداً صحيحاً N و نَقسِم الأرقام المُكوِّنة له إلى مجموعات كل مجموعة

مؤلَّفة من ثلاثة أرقام ابتداءً من خانة الآحاد:

$$N = a_{3k+2}a_{3k+1}a_{3k}\cdots a_5a_4a_3a_2a_1a_0$$
$$= a_{3k+2}a_{3k+1}a_{3k}\times 1000^k + \cdots + a_5a_4a_3\times 1000 + a_2a_1a_0$$

حيث $0\le a_i \le 9$ لجميع القيم i. بما أن $1000\equiv 1 \bmod 27$ فإن

$$N \equiv a_{3k+2}a_{3k+1}a_{3k} + \cdots + a_5a_4a_3 + a_2a_1a_0 \bmod 27$$

هذا يقتضي أن N يقبل القسمة على 27 إذا وفقط إذا كان مجموع الأرقام المُكوِّنة للعدد N مأخوذاً على شكل مجموعات ثلاثية، ومبتدئاً من خانة الآحاد، يقبل القسمة على 27. فعلى سبيل المثال

$$6615 \equiv 6+615 = 621 \equiv 0 \bmod 27$$
$$573118 \equiv 573+118 = 691 \equiv 16 \bmod 27$$

أي أن $27|6615$ و $27 \nmid 573118$.

80. ندرس الحالتين المحتملتين لقيمة n. إذا كان $n=2k$ عدداً زوجياً فسوف نحصل على

$$4\cdot 14^{2k}+1 \equiv 4(-1)^{2k}+1 \equiv 5 \equiv 0 \bmod 5$$

وإذا كان $n=2k+1$ عدداً فردياً فسوف نحصل على

$$4\cdot 14^{2k+1}+1 \equiv 1\cdot(-1)^{2k+1}+1 \equiv 0 \bmod 3$$

أي أن $5|4\cdot 14^n+1$ إذا كان n عدداً زوجياً و $3|4\cdot 14^n+1$ إذا كان n عدداً فردياً. هذا يقتضي أن أي عدد على الصورة $4\cdot 14^n+1$ هو عدد مؤلف.

81. نلاحظ أولاً أن العبارة صحيحة إذا كان $r=1$. لذا نفرض أن $r>1$. إذا كان $p=2$ فإن

$$\binom{2r}{2}-r=2r(r-1)$$

ومن ثم $\binom{2r}{2}\equiv r \mod 2$. الآن نفرض أن $p>2$. بما أن

$$(p-1)!\binom{rp}{p}=r(rp-1)(rp-2)\cdots(rp-(p-1))$$

و

$$\begin{aligned}(rp-1)(rp-2)\cdots(rp-(p-1))&\equiv(-1)(-2)\cdots(-(p-1))\\&\equiv(p-1)! \mod p\end{aligned}$$

إذاً $(p-1)!\binom{rp}{p}\equiv r\cdot(p-1)! \mod p$. هـــــذا يقتـــــضي أن $\binom{rp}{p}\equiv r \mod p$ لأن $(p,(p-1)!)=1$.

82. بملاحظة أن

$$\binom{p^r}{k}=\frac{(p^r)!}{k!\cdot(p^r-k)!}=\frac{p^r\cdot(p^r-1)!}{k\cdot(k-1)!\cdot(p^r-k)!}=\binom{p^r-1}{k-1}\frac{p^r}{k}$$

يمكننـا أن نكتـب $p^r\binom{p^r-1}{k-1}=\binom{p^r}{k}k$. بـما أن $1\le k\le p^r-1$، إذاً $(k,p^r)=p^t$ حيث أن القـيم المحتملـة لـلأس t هـي $0,1,2,\cdots,r-1$. هذا يقتضي أن $p^{r-1}\binom{p^r-1}{k-1}\mid k$ ومـن ثـم فالعـدد $\binom{p^r-1}{k-1}\frac{p^{r-1}}{k}$ هـو عدد صحيح. نستنتج من ذلك أن

$$\binom{p^r}{k}=\binom{p^r-1}{k-1}\frac{p^{r-1}}{k}\times p\equiv 0 \mod p$$

83. إذا كان $a\equiv 1 \mod m^k$ فإنه يمكننا أن نكتـب $a=1+m^kt$،

حيث t عدد صحيح. هذا يعطينا الآتي:

$$\begin{aligned} a^m &= (1+m^k t)^m \\ &= 1+\binom{m}{1}m^k t+\binom{m}{2}(m^k t)^2+\cdots+\binom{m}{m}(m^k t)^m \\ &\equiv 1 \bmod m^{k+1} \end{aligned}$$

84. حيث إنَّ $936=8\times9\times13$ و $(n,936)=1$ فإن $(n,8)=(n,9)=(n,13)=1$. باستخدام نتيجة 19 نحصل على التطابق

$$n^{13}\equiv n \bmod 13$$

بملاحظة أن $\phi(9)=6$ فباستخدام نظرية أويلر نحصل على $n^6\equiv 1 \bmod 9$. بتربيع الطرفين نحصل على $n^{12}\equiv 1 \bmod 9$. بضرب الطرفين في n نحصل على التطابق

$$n^{13}\equiv n \bmod 9$$

بنفس الطريقة نجد أن $n^4=n^{\phi(8)}\equiv 1 \bmod 8$. بتكعيب الطرفين ومن ثم ضرب الطرفين في n نحصل على التطابق

$$n^{13}\equiv n \bmod 8$$

من التطابقات الثلاث أعلاه نستنتج أن $n^{13}\equiv n \bmod [8,9,13]$، أو $n^{13}\equiv n \bmod 936$، أي أن $936|n^{13}-n$.

85. لنفرض أن $19|n^2+4$. إذاً $n^2\equiv -4 \bmod 19$. هذا يقتضي أن $n^{18}\equiv -4^9 \bmod 19$. وحيث إنَّ $(n,19)=(-4,19)=1$ و $4^9\equiv(4^2)^4\cdot4\equiv(-3)^4\cdot4\equiv5\cdot4\equiv1 \bmod 19$، إذاً $n^{18}\equiv -1 \bmod 19$، وهذا مستحيل لأنه يناقض نظرية فيرما (

$n^{18} \equiv 1 \bmod 19$). نستنتج من ذلك أن $19 \nmid n^2 + 4$.

86. لاحظ أولاً أن $a^n - a$ عدد زوجي. إذاً $a^n \equiv a \bmod 2$. نقوم الآن بإثبات أن $a^n \equiv a \bmod 3$. إذا كان $3|a$ فإن $a^n \equiv a \bmod 3$. لنفرض أن $(a,3)=1$ و لنكتب $n = 2k+1$ حيث $k \geq 0$ عدد صحيح. باستخدام نظرية فيرما، نجد أن $a^2 \equiv 1 \bmod 3$. بالرفع إلى الأس k ومن ثم ضرب الطرفين بالعدد a نحصل على $a^n = a^{2k+1} \equiv a \bmod 3$. إذاً $a^n \equiv a \bmod 3$ لأي عدد صحيح a وأي عدد فردي n. نستنتج من ذلك أن $a^n \equiv a \bmod [2,3]$، أي أن $a^n \equiv a \bmod 6$.

87. إذا كان $p | 1 + n + \cdots + n^{p-2}$، فلابد أن يكون $p \nmid n$ (وإلا سوف نحصل على $p | 1$، وهذا تناقض). باستخدام نظرية فيرما يصبح لدينا $n^{p-1} \equiv 1 \bmod p$، أي أن $p | n^{p-1} - 1$. بما أن

$$n^{p-1} - 1 = (n-1)(1 + n + \cdots + n^{p-2}) ....(*)$$

فإننا نستنتج أنه إما $p | n - 1$ أو $p | 1 + n + \cdots + n^{p-2}$. باستخدام السؤال رقم 31، نجد أن $(n-1, p-1) = \left(\dfrac{n^{p-1}-1}{n-1}, n-1\right)$. نستنتج من ذلك أنه إذا كان $p \left| \dfrac{n^{p-1}-1}{n-1} \right.$، فإن $p \nmid n-1$ (وإلا سوف نحصل على $p | (n-1, p-1)$ ومن ثم $p | p-1$، وهذا تناقض). إذاً إذا كان $p | 1 + n + \cdots + n^{p-2}$، فإن $n \not\equiv 0,1 \bmod p$. والعكس أيضاً صحيح: إذا كان $n \not\equiv 0 \bmod p$، فإن $n^{p-1} \equiv 1 \bmod p$ (بواسطة نظرية فيرما). وإذا كان $n \not\equiv 1 \bmod p$، فإنه من (*) ينتج $p | 1 + n + \cdots + n^{p-2}$. نستنتج من ذلك أن قيم n الصحيحة التي تحقق شرط السؤال هي $n \not\equiv 0,1 \bmod p$.

88. بما أن $p-2$ عدد فردي فإن $a^{p-2} \equiv -(p-a)^{p-2} \bmod p$،
أو $a^{p-2}+(p-a)^{p-2} \equiv 0 \bmod p$. هذا يقتضي أن

$$\begin{aligned}
&1^{p-2}+2^{p-2}+\cdots+(p-1)^{p-2}\\
&\equiv [1^{p-2}+(p-1)^{p-2}]+\cdots+\left[\left(\frac{p-1}{2}\right)^{p-2}+\left(p-\frac{p-1}{2}\right)^{p-2}\right] \bmod p\\
&\equiv 0 \bmod p
\end{aligned}$$

89. نقوم بحساب $1117^{2228^{3339}}$ قياس 10. لنضع $A=2228^{3339}$.
لاحظ أولاً أن $1117 \equiv 7 \bmod 10$ و $\phi(10)=4$ و $A \equiv 0 \bmod 4$،
أي $A=4k$، حيث k عدد صحيح موجب. باستخدام نظرية أويلر نحصل على $7^{\phi(10)}=7^4 \equiv 1 \bmod 10$ ومن ثم

$$1117^{2228^{3339}}=1117^{A} \equiv 7^{4k} \equiv 1^{k} \equiv 1 \bmod 10$$

هذا يقتضي أن الرقم الموجود في منزلة الآحاد للعدد $1117^{2228^{3339}}$ يساوي 1.

90. لإيجاد الأرقام الموجودة في منزلتي الآحاد و العشرات للعدد $13^{14^{15}}$ نقوم بحساب هذا العدد قياس 100. بما أن $\phi(100)=40$ فباستخدام نظرية أويلر نجد أن $13^{40} \equiv 1 \bmod 100$. لنضع $A=14^{15}$.
نحسب A قياس 5 و 8:

$$A=14^{15} \equiv (-1)^{15} \equiv 4 \bmod 5$$
$$A=14^{15} \equiv (-2)^{15} \equiv 0 \bmod 8$$

باستخدام نظرية الباقي الصينية نجد أن $A \equiv 24 \bmod 40$، أي أن
$A=24+40k$ حيث k عدد صحيح موجب. هذا يقتضي أن

$$13^{14^{15}}=13^{A}=13^{24+40k} \equiv 13^{24} \bmod 100$$

لكن

$$13^{24}=169^{12}\equiv(-31)^{12}=961^{6}\equiv 61^{6}=3721^{3}\equiv 21^{3}$$
$$=9261\equiv 61 \bmod 100$$

هذا يقتضي أن $13^{14^{15}}\equiv 61 \bmod 100$ ومن ثم فإن الـرقمين الموجـودين في منزلتي الآحاد و العشرات للعدد $13^{14^{15}}$ هما 61.

91. المطلوب هو إيجاد عدد صحيح موجب b يحقق $0\le b<1000$ و $3^{9997}\equiv b \bmod 1000$. بما أن $\phi(1000)=400$، إذاً باستخدام نظرية أويلر نحصل على $3^{400}\equiv 1 \bmod 1000$ ومن ثـم $3^{10000}\equiv 1 \bmod 1000$. أيضاً $3^{10000}\equiv 27b \bmod 1000$. هـذا يقتضي أن $27b\equiv 1 \bmod 1000$. نقـوم بحـل هـذا التطـابق الخطـي بتحويلـه إلى معادلـة ديوفانتيـة خطيـة $27b+1000k=1$. باسـتخدام خوارزميـة أُقليـدس نجـد بسـهولة أن $b\equiv 37 \bmod 1000$. نستنتج من ذلك أن آخر ثلاثة أرقام للعدد 3^{9997} هي .037

92. من فـرض السـؤال نسـتنتج أولاً أن $(n,2)=1$. لنفـرض أن n عدد أولي. باستخدام نظرية فيرما نحصـل عـلى التطـابق $2^{n-1}\equiv 1 \bmod n$. بضرب التطابق المعطى $2^{n-2}\equiv 1 \bmod n$ بالعدد 2 نحصـل عـلى التطـابق $2^{n-1}\equiv 2 \bmod n$ ومن ثم $1\equiv 2 \bmod n$، أي أن $n\mid 1$، وهـذا مسـتحيل لأن $n>2$. نستنتج من ذلك أن n عدد مؤلف.

93. إذا كان $2^{p-1}\equiv 1 \bmod p^{2}$ فإنه برفـع طـرفي التطـابق إلى الأُس $p+1$ نحصـــل عـــلى $2^{p^{2}-1}\equiv 1 \bmod p^{2}$. الآن لِنفـــرض أن $2^{p^{2}-1}\equiv 1 \bmod p^{2}$. هذا يقتضي أن $p^{2}\mid 2^{p^{2}-1}-1$. نُكوِن المتطابقة التالية:

$$2^{p^2-1}-1=2^{(p-1)(p+1)}-1=(2^{p-1}-1)(2^{p(p-1)}+\cdots+2^{2(p-1)}+2^{p-1}+1)$$

باستخدام نظرية فيرما نحصل على

$$\begin{aligned}2^{p(p-1)}+\cdots+2^{2(p-1)}+2^{p-1}+1 &\equiv 1+\cdots+1+1+1 \bmod p\\ &\equiv p+1\equiv 1 \bmod p\end{aligned}$$

أي أن $(2^{p(p-1)}+\cdots+2^{2(p-1)}+2^{p-1}+1,p)=1$. الآن حيث إنَّ $p^2 \mid 2^{p^2-1}-1$ و $(2^{p(p-1)}+\cdots+2^{2(p-1)}+2^{p-1}+1,p^2)=1$ فإن $p^2 \mid 2^{p-1}-1$، أي أن $2^{p-1}\equiv 1 \bmod p^2$ وبهذا يتم الإثبات.

94. حيث إنَّ $\phi(2^n)=2^{n-1}$ و $(2^n,5)=1$ فباستخدام نظرية أويلر نحصل على التطابق $5^{\phi(2^n)}\equiv 1 \bmod 2^n$، أي $5^{2^{n-1}}\equiv 1 \bmod 2^n$. هذا يقتضي أن $5^{2^{n-1}}=1+2^n a_n$ حيث a_n عدد صحيح موجب.

95. بواسطة نظرية ولسون $p\mid (p-1)!+1$ وبملاحظة أن $k \nmid (p-1)!+1$ لجميع القيم $2\le k\le p-1$، نستنتج أن $(p!,(p-1)!+1)=p$.

96. التطابق $(2n-3)!\equiv 0 \bmod 2n$ مُتحقق عندما $n=3$. لنفرض أن $n>3$. إذاً $2n-3>2$ و $2n-3>n$ (لأن $n>3$). هذا يعني أن العددين 2 و n يظهران كحدّين في المضروب $(2n-3)!$، أي أن $2n \mid (2n-3)!$ ومن ثم $(2n-3)!\equiv 0 \bmod 2n$.

97. نستخدم نظرية ولسون: $(p-1)!\equiv -1 \bmod p$. نُعيد كتابة التطابق السابق على النحو الآتي:

$$1\cdot 2\cdot 3\cdots(p-k)\cdot(p-k+1)\cdot(p-k+2)\cdots$$
$$(p-k+k-1)\equiv -1 \bmod p$$

بإيجاد قيمة الحدود الأخيرة قياس p، نحصل على

$$(p-k)!\cdot(-(k-1))\cdot(-(k-2))\cdots(-1)\equiv -1 \bmod p$$

وبالتبسيط يصبح لدينا

$$(p-k)!\cdot(-1)^{k-1}\cdot(k-1)!\equiv -1 \bmod p$$

وبالقسمة على $(-1)^{k-1}$ نحصل على المطلوب

$$(p-k)!\cdot(k-1)!\equiv(-1)^{k} \bmod p$$

98. بأخذ $n=p-4$، حيث $p\geq 5$ عدد أولي، نجد أن $(n+3)!+1=(p-1)!+1$ يقبل القسمة على p وذلك باستخدام نظرية ولسون.

99. بأخذ $n=p-1$، حيث $p\geq 3$ عدد أولي، وباستخدام نظرية فيرما، نجد أن

$$n\times 2^{n}+1=(p-1)\times 2^{p-1}+1\equiv(-1)\times 1+1\equiv 0 \bmod p$$

أي أن p يقسم $n\times 2^{n}+1$.

100. نلاحظ أولاً أن المعادلة $(p-1)!+1=p^{k}$ مُتحققة في الحالات التالية $(p,k)=(2,1),\ (3,1),\ (5,2)$. لذا نفرض فيما يلي أن $p>5$. بكتابة المعادلة على الشكل $(p-1)!=p^{k}-1$ وبالقسمة على $p-1$ نحصل على المعادلة الآتية:

$$(p-2)!=p^{k-1}+p^{k-2}+\cdots+p+1$$

نُعيد كتابة المعادلة السابقة على الصورة الآتية:

$$(p-2)!=(p^{k-1}-1)+(p^{k-2}-1)+\cdots+(p-1)+k$$

بما أن $p>5$ فإن $p-1|(p-2)!$ (مثال 24). أيضاً $p-1|p^i-1$ لجميع قيم $1\le i\le k-1$. هذا يقتضي أن $p-1|k$ ومن ثم $k\ge p-1$. لكن مثل هذه القيمة k لن تُحقق المعادلة $(p-1)!+1=p^k$ وذلك لأن $p^k=(p-1)!+1<p^{p-2}+1$ أو $p^{p-2}(p^{k-(p-2)}-1)<1$ وهذا مستحيل. إذاً المعادلة $(p-1)!+1=p^k$ غير متحققة إذا كان $p>5$. (ملاحظة: استخدمنا أعلاه العلاقة التالية: $(p-1)!=2\cdot 3\cdots\cdot(p-1)<\underbrace{p\cdot p\cdots\cdot p}_{p-2}=p^{p-2}$).

101. من مُعطى السؤال نجد أن

$$a=(p-1)!\left[1+\frac{1}{2}+\frac{1}{3}+\cdots+\frac{1}{p-1}\right]=\sum_{k=1}^{p-1}\frac{(p-1)!}{k}$$

بما أن $(p-1)!\equiv -1 \bmod p$ و $k^{p-1}\equiv 1 \bmod p$ حيث $1\le k\le p-1$ نستنتج أن $(p-1)!\equiv -k^{p-1} \bmod p$. لكن $(k,p)=1$. إذاً

$$\frac{(p-1)!}{k}\equiv -k^{p-2} \bmod p$$

هذا يقتضي أن

$$a=\sum_{k=1}^{p-1}\frac{(p-1)!}{k}\equiv\sum_{k=1}^{p-1}-k^{p-2}\equiv 0 \bmod p$$

حيث إن التطابق الأخير ناتج من سؤال رقم 88.

102. نُريد أن نُثبت أن $3^{120}\equiv 1 \bmod 121$. بما أن $\phi(121)=\phi(11^2)=11(11-1)=110$ فباستخدام نظرية أويلر نحصل

علـــــى $3^{110} \equiv 1 \bmod 121$ أيضـــــــاً مـــــــن العلاقـــــــة $3^5 = 243 = 121 \times 2 + 1 \equiv 1 \bmod 121$ نســتنتج أن $3^{10} \equiv 1 \bmod 121$ بضرب التطابقين السابقين نحصل علـى $3^{120} \equiv 1 \bmod 121$، أي أن 121 عدد شبه أولي للأساس 3.

103. نُريد أن نُثبت أن $2^{n-1} \equiv 1 \bmod n$. نُلاحظ أولاً مايلي:

$$n-1 = \frac{2^{2p}-1}{3} - 1 = \frac{4(2^{2p-2}-1)}{3} = \frac{4(2^{p-1}-1)(2^{p-1}+1)}{3}$$

بـما أن $2^{p-1} \equiv 1 \bmod p$ (نظريـة فيرمـا) و $2^{p-1} \equiv 1 \bmod 3$ (لأن $p-1$ عدد زوجي)، فإن $2^{p-1} \equiv 1 \bmod 3p$ (لأن $(3,p)=1$). هـذا يقتضي أن $3p \mid 2^{p-1}-1$ ومـن ثـم $4p \mid n-1$ (باسـتخدام المعادلـة أعـلاه) أو $2p \mid n-1$. لكـن إذا كـان $2p \mid n-1$ فـإن $2^{2p}-1 \mid 2^{n-1}-1$. بـما أن $3n = 2^{2p}-1$ فـــإن $3n \mid 2^{n-1}-1$ ومــــن ثـــم $n \mid 2^{n-1}-1$، أي أن $2^{n-1} \equiv 1 \bmod n$ وهو المطلوب.

104. حيــث إنَّ $p \neq 3$ فــإن $(3,5p)=1$. نُريــد أن نُثبِــت أن $3^{5p-1} \not\equiv 1 \bmod 5p$. نبــدأ بالحالـــة $p=2$. نجـــد بســـهولة أن $3^9 = 3 \times 3^4 \times 3^4 \equiv 3 \times 1 \times 1 \equiv 3 \bmod 10$، أي أن $3^9 \not\equiv 1 \bmod 10$ ومن ثم فإن العدد 10 ليس عدداً شبه أولي للأساس 3.

نأخـذ الآن الحالـة $p=5$. باسـتخدام نظريـة أويلـر نجـد أن $3^{\phi(25)} \equiv 1 \bmod 25$، أي أن $3^{20} \equiv 1 \bmod 25$. هـــذا يقتـــضي أن $3^{24} = 3^4 \times 3^{20} \equiv 6 \times 1 = 6 \bmod 25$، أي أن 25 لـيس عـدداً شـبه أولي للأساس 3.

الآن نفـرض أن $p > 5$. أيضـاً باسـتخدام نظريـة أويلـر نجـد أن

$3^{\phi(5p)} \equiv 1 \bmod 5p$، أي أن $3^{4(p-1)} \equiv 1 \bmod 5p$. بضرب طرفي التطابق السابق بالعدد 3^{p+3} نحصل على التطابق

$$3^{5p-1} \equiv 3^{p+3} \bmod 5p$$

لإكمال الإثبات نُثبِت أن $3^{p+3} \not\equiv 1 \bmod 5p$: إذا كان $3^{p+3} \equiv 1 \bmod 5p$ فإن $3^{p+3} \equiv 1 \bmod p$ ومن ثم (باستخدام نتيجة 19) $3 \times 3^3 \equiv 1 \bmod p$. هذا يقتضي أن $p \mid 80 = 2^4 \times 5$ ومن ثم $p = 2$ أو $p = 5$ وهذا تناقض لأن $p > 5$. إذاً $3^{p+3} \not\equiv 1 \bmod 5p$ ومن ثم

$$3^{5p-1} \not\equiv 1 \bmod 5p$$

أي أن العدد $5p$ ليس عدداً شبه أولي للأساس 3.

105. لكي نُثبِتَ أن p^2 ليس عدداً كارمايكيلياً نحتاج أن نجِد عدداً صحيحاً a يُحقق $(a,p^2)=1$ و $a^{p^2-1} \not\equiv 1 \bmod p^2$. نأخذ العدد $a = p+1$. من الواضح أن $(p+1,p^2)=1$. أيضاً من العلاقة

$$(p+1)^{p^2-1} - 1 = \sum_{i=0}^{p^2-1} \binom{p^2-1}{i} p^i - 1 = -p + p^3 + \sum_{i=2}^{p^2-1} \binom{p^2-1}{i} p^i$$

نلاحظ أن جميع الحدود في الطرف الأيمن تقبل القسمة على p^2 ماعدا الحد الأول. نستنتج من ذلك أن $p^2 \nmid (p+1)^{p^2-1} - 1$، أي أن $(p+1)^{p^2-1} \not\equiv 1 \bmod p^2$. هذا يُثبت أن p^2 ليس عدداً كارمايكيلياً.

106. بما أن $(2,p)=1$ فإنه يوجد حل وحيد للتطابق $2x \equiv 1 \bmod p$. بكتابة التطابق السابق على الشكل

$$2x \equiv 1 \equiv p+1 \bmod p$$

وبملاحظة أن $p+1$ عدد زوجي فإننا نحصل على الحل

$x \equiv \frac{p+1}{2} \mod p$. (لاحظ أن $1 < \frac{p+1}{2} < p$). من ذلك نستنتج أن المعكوس الضربي قياس p للعدد 2 هو العدد $\frac{p+1}{2}$).

107. السؤال يُكافئ إيجاد أصغر عدد صحيح موجب يُحقق النظام

$$x \equiv 4 \mod 5$$
$$x \equiv 5 \mod 6$$
$$x \equiv 6 \mod 7$$

التطابق الأول يقتضي أن $x = 4 + 5k$. بالتعويض في التطابق الثاني ثم حله نجد أن $k = 5 + 6l$. بالتعويض في التطابق الثالث ثم حله نجد أن $l = 6 + 7t$. هذا يقتضي أن

$$x = 4 + 5k = 29 + 30l = 209 + 210t$$

حيث t عدد صحيح. إذاً أصغر عدد صحيح موجب يُحقق السؤال هو $x = 209$ (عندما $t = 0$).

108. نُكوِن نظام التطابقات الآتي:

$$x \equiv 0 \mod p_1$$
$$x + 1 \equiv 0 \mod p_2^2$$
$$x + 2 \equiv 0 \mod p_3^3$$
$$\vdots$$
$$x + r - 1 \equiv 0 \mod p_r^r$$

حيث إنَّ الأعداد $p_1, p_2^2, \cdots, p_r^r$ أعداد أولية نسبياً مثنى مثنى، فإنه، باستخدام نظرية الباقي الصينية، يوجد للنظام أعلاه حل وحيد N_0 قياس $P = p_1 p_2^2 \cdots p_r^r$. لذا فالأعداد المطلوبة هي $N \equiv N_0 \mod p_1 p_2^2 \cdots p_r^r$.

109. نلاحـظ أولاً أن $123=3\times 41$. بـما أن $3|231$ و $3|312$، فإن $A=(231^{132}+312^{213})^{321}$ يقبل القسمة على 3، أي أن

$$A\equiv 0 \bmod 3..............(1)$$

بما أن $231\equiv 26 \bmod 41$ و $312\equiv 25 \bmod 41$، إذاً

$$A\equiv (26^{132}+25^{213})^{321} \bmod 41$$

باستخدام نظرية فيرما نحصل على $26^{40}\equiv 1 \bmod 41$. هـذا يعطينا $26^{120}\equiv 1 \bmod 41$ ومـن ثـم $26^{132}\equiv 26^{12} \bmod 41$. لكـن $26^{12}\equiv 20^{6}\equiv 31^{3}\equiv 25 \bmod 41$. إذاً $26^{132}\equiv 25 \bmod 41$.

أيضاً باستخدام نظرية فيرما نحصل على $25^{40}\equiv 1 \bmod 41$. هـذا يعطينا $25^{200}\equiv 1 \bmod 41$ ومـن ثـم $25^{213}\equiv 25^{13} \bmod 41$. لكـن $25^{13}\equiv 25(10)^{6}\equiv 25(10)\equiv 4 \bmod 41$. إذاً $25^{213}\equiv 4 \bmod 41$. نستنتج من ذلك أن

$$A\equiv (25+4)^{321}\equiv 29^{321} \bmod 41$$

باستخدام نظرية فيرما نحصل على $29^{321}=29\times (29^{40})^{8}\equiv 29\times 1\equiv 29 \bmod 41$. أي أن

$$A\equiv 29 \bmod 41............(2)$$

باستخدام نظرية الباقي الصينية نستنتج من (1) و (2) أن $A\equiv 111 \bmod 123$. إذاً باقي قسمة A على 123 يساوي 111.

110. لِنضع $x=4^{1111}$. لاحـظ أولاً أن $1155=3\times 5\times 7\times 11$. نجد بسهولة أن

$$x \equiv 1 \equiv 4 \bmod 3$$
$$x \equiv 4 \bmod 5$$
$$x \equiv 4 \bmod 7$$
$$x \equiv 4 \bmod 11$$

هـذا يقتــضي أن $x \equiv 4 \bmod [3,5,7,11]$ أو $x \equiv 4 \bmod 1155$
ومن ثم فإن باقي قسمة 4^{1111} على 1155 يساوي 4.

111. لنكتب $(a,b)=d$. إذاً التطابق $ax \equiv 0 \bmod b$ قابل للحل و عدد حلوله يساوي d. نستنتج مـن ذلـك أن عـدد الأعـداد الموجـودة في المجموعــة $\{a,2a,3a,\cdots,ba\}$ التـي تقبـل القســمة عــلى b يســاوي $(a,b)=d$.

112. بملاحظـــة أن $143=11\times13$، نســـتنتج أن التطـــابق $17x \equiv 2 \bmod 143$ يكافئ النظام

$$\begin{cases} 17x \equiv 2 \bmod 11 \\ 17x \equiv 2 \bmod 13 \end{cases}$$

حــل التطــابق الأول هــو $x \equiv 4 \bmod 11$ وحــل التطــابق الثــاني هــو $x \equiv 7 \bmod 13$. بتكوين النظام

$$\begin{cases} x \equiv 4 \bmod 11 \\ x \equiv 7 \bmod 13 \end{cases}$$

نجد أن الحل، باستخدام نظرية الباقي الصينية، هو $x \equiv 59 \bmod 143$.

113. حيـــــث إنَّ $24=3\times8$، فـــــإن التطـــــابق $x^3+2x^2-x-2 \equiv 0 \bmod 24$ يكافئ النظام

$$\begin{cases} x^3+2x^2-x-2\equiv 0 \bmod 3 \\ x^3+2x^2-x-2\equiv 0 \bmod 8 \end{cases}$$

يوجد حلان للتطابق الأول هما $x\equiv -1, 1 \bmod 3$ وثلاثة حلول للتطابق الثاني هي $x\equiv -2, -1, 1 \bmod 8$. هذه الحلول تعطينا ستة أنظمة خطية:

$$\begin{cases} x\equiv -1 \bmod 3,\ x\equiv -2 \bmod 8 \\ x\equiv -1 \bmod 3,\ x\equiv -1 \bmod 8 \\ x\equiv -1 \bmod 3,\ x\equiv 1 \bmod 8 \\ x\equiv 1 \bmod 3,\ x\equiv -2 \bmod 8 \\ x\equiv 1 \bmod 3,\ x\equiv -1 \bmod 8 \\ x\equiv 1 \bmod 3,\ x\equiv 1 \bmod 8 \end{cases}$$

حلول هذه الأنظمة الخطية هي:

$$x\equiv 1,\ 7,\ 14,\ 17,\ 22,\ 23 \bmod 24$$

وهي نفسها حلول التطابق المعطى.

114. حيث إنَّ $95=5\times 19$، فإن التطابق $2x^3+x^2-1\equiv 0 \bmod 95$ يكافئ النظام الآتي:

$$\begin{cases} 2x^3+x^2-1\equiv 0 \bmod 5 \\ 2x^3+x^2-1\equiv 0 \bmod 19 \end{cases}$$

بما أنه لا يوجد حل للتطابق الأول في النظام أعلاه، إذاً لا يوجد أي حل للتطابق $2x^3+x^2-1\equiv 0 \bmod 95$.

115. في النظام

$$\begin{cases} 2x^3 - x^2 - 1 \equiv 0 \bmod 3 \\ 4x \equiv 2 \bmod 10 \end{cases}$$

حل التطابق الأول هو $x \equiv 1 \bmod 3$، بينما للتطابق الثاني الحلان $x \equiv 3,8 \bmod 10$. نستخدم هذه الحلول لتكوين نظامين خطيين:

$$\begin{cases} x \equiv 1 \bmod 3,\ x \equiv 3 \bmod 10 \\ x \equiv 1 \bmod 3,\ x \equiv 8 \bmod 10 \end{cases}$$

حل النظام الأول هو $x \equiv 13 \bmod 30$ و حل النظام الثاني هو $x \equiv 28 \bmod 30$. إذاً للنظام المعطى حلان هما $x \equiv 13,\ 28 \bmod 30$.

116. لاحظ أن أي حل للتطابق

$$x^2 + 1 \equiv 0 \bmod 169 \ ....(1)$$

هو أيضاً حل للتطابق

$$x^2 + 1 \equiv 0 \bmod 13 \ ....(2)$$

حلول التطابق (2) هي $x \equiv -5 \bmod 13$ و $x \equiv 5 \bmod 13$. هذا يقتضي أن أي حل للتطابق (1) يجب أن يكون على إحدى الصورتين الآتيتين

$$\begin{cases} x = -5 + 13t \\ x = 5 + 13u \end{cases}$$

حيث $t, u \in \mathbb{Z}$. بتعويض هذين الحلين في التطابق (1) نحصل على التطابقين الخطيين الآتيين

$$\begin{cases} 26 - 130t \equiv 0 \bmod 169 \\ 26 + 130u \equiv 0 \bmod 169 \end{cases}$$

بالقسمة على 13 نحصل على

$$\begin{cases} 2-10t \equiv 0 \mod 13 \\ 2+10u \equiv 0 \mod 13 \end{cases}$$

والتي حلولهما على التوالي هي $t \equiv 8 \mod 13$ و $u \equiv 5 \mod 13$، أي أن

$$\begin{cases} t = 8+13k \\ u = 5+13l \end{cases}$$

حيث $k, l \in \mathbb{Z}$. هذا يقتضي أن

$$\begin{cases} x = 99+169k \\ x = 70+169l \end{cases}$$

ومن ثم فإن حلول التطابق (1) هي $x \equiv 99 \mod 169$ و $x \equiv 70 \mod 169$.

117. لاحظ أولاً أن $x^7 \equiv x \mod 7$ (نتيجة 19). هذا يقتضي أن $x^{15} \equiv x^3 \mod 7$. إذاً التطابق $x^{15} - 2x - 4 \equiv 0 \mod 7$ يكافئ التطابق $x^3 - 2x - 4 \equiv 0 \mod 7$ الذي له الحل الوحيد $x \equiv 2 \mod 7$.

118. حيث إنَّ $a^p \equiv a \mod p$ لجميع الأعداد الصحيحة a (نتيجة 19)، إذاً للتطابق $x^p - x \equiv 0 \mod p$ عدد p من الحلول هي $x \equiv 0,1,2,\cdots,p-1 \mod p$.

119. نبدأ الحل بملاحظة أن $x^p \equiv x \mod p$ لأي عدد صحيح x (نتيجة 19). برفع طرفي التطابق إلى الأُس p نجد أن $x^{p^2} \equiv x^p \equiv x \mod p$. برفع طرفي المتطابق السابق إلى الأُس p نحصل على التطابق $x^{p^3} \equiv x^p \equiv x \mod p$. بتكرار هذه العملية نجد أن

$x^{p^n} \equiv x \mod p$. هـذا يقتضي أن التطـابق $x^{p^n} \equiv a \mod p$ مكـافئ للتطابق $x \equiv a \mod p$، أي أن حل التطابق المعطى هو $x \equiv a \mod p$.

120. لِنكتب كثيرة الحدود المُعطاة في السؤال على الشكل التالي:

$$f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0$$

حيث $n \geq 1$ و المُعـاملات $a_0, a_1, \cdots, a_n$ أعـداد صـحيحة. إذا كـان $a_0 = 0$، فإن التطابق $f(x) \equiv 0 \mod p$ قابل للحـل لأي عـدد أولي p (أحد الحلول هو $x \equiv 0 \mod p$). لذا لنفرض أن $a_0 \neq 0$. لنفـرض الآن أن التطابق $f(x) \equiv 0 \mod p$ قابل للحل لعدد محدود فقط مـن الأعـداد الأولية $p_1, p_2, \cdots, p_r$. لنُعرف العدد $b = a_0^2 p_1 p_2 \cdots p_r$. هذا يُعطينا

$$f(b) = a_0(1+B)$$

حيث

$B = a_1 a_0 (p_1 \cdots p_r) + a_2 a_0^3 (p_1 \cdots p_r)^2 + \cdots + a_n a_0^{2n-1} (p_1 \cdots p_r)^n$.
بإمكاننـــا أن نختـــار عـــدداً أوليـــاً q بحيـــث $q \mid 1+B$ و $q \nmid a_0$ (لأن $(a_0, 1+B) = 1$). هذا يقتضي أولاً أن التطابق

$$f(x) \equiv 0 \mod q$$

قابل للحل (أحد الحلـول هـو $x \equiv b \mod q$)، وثانيـاً $q \neq p_i$ لجميـع القـــيم $1 \leq i \leq r$ (لأن $q \mid 1+B$ و $q = p_i$ لإحـــدى القـــيم $1 \leq i \leq r$ يقتضي أن $q \mid 1$ وهذا تناقض). هـذا يُنـاقض مـا افترضـناه مـن أن التطـابق $f(x) \equiv 0 \mod p$ قابل للحل فقط للأعداد الأولية $p_1, p_2, \cdots, p_r$. من هذا التناقض نسـتنتج أن التطـابق $f(x) \equiv 0 \mod p$ قابـل للحـل لعـدد لانهائي من الأعداد الأولية p.

121. لاحظ أولاً (من حل مثال 35) أن

$$F_n - 2 = F_0 F_1 F_2 \cdots F_{n-1}$$

بإضافة 3 للطرفين وملاحظة أن $F_0 = 3$ نجد أن

$$F_n + 1 = F_0 F_1 F_2 \cdots F_{n-1} + 3 = 3(F_1 F_2 \cdots F_{n-1} + 1)$$

بما أن $F_1 F_2 \cdots F_{n-1} + 1$ عدد زوجي، نستنتج أن $F_n + 1 = 6k$ ومن ثم $F_n = 6k - 1$.

122. من مثال 36، نستنتج أن عدد الخانات العشرية لعدد فيرما $F_n = 2^{2^n} + 1$ يساوي عدد الخانات العشرية للعدد $F_n - 1 = 2^{2^n}$. إذاً عدد الخانات العشرية لعدد فيرما F_{21} يساوي $\left[\!\left[\log_{10} 2^{2^{21}} \right]\!\right] + 1 = 631306$.

123. إذا كان $n \geq 2$ فإن العدد الموجود في خانة الآحاد لعدد فيرما $F_n = 2^{2^n} + 1$ يساوي 7 (مثال 36). أيضاً $F_0 = 3$ و $F_1 = 5$. نستنتج من ذلك أن عدد فيرما لا يمكن أن يكون مربعاً كاملاً (لأن الأعداد المحتملة التي يمكن أن توجد في خانة الآحاد للمربع الكامل هي 0, 1, 4, 5, 6, 9) ومن ثم لا يمكن أن يساوي عدداً مرفوعاً لأُسٍ زوجي.

لنفرض الآن أن $F_n = x^m$ حيث m و $x > 1$ عددان فرديان. إذاً

$$2^{2^n} = x^m - 1 = (x-1)(x^{m-1} + x^{m-2} + \cdots + x + 1)$$

إذا كان $m > 1$ فمن المعادلة أعلاه نستنتج أن العدد الفردي $x^{m-1} + x^{m-2} + \cdots + x + 1$ يقسم العدد 2^{2^n} وهذا مستحيل. إذاً لابد أن يكون $m = 1$. هذا يعني أنه في كلتا الحالتين عدد فيرما لا يساوي قوة لأي عددٍ صحيح.

124. بما أن $F_n = 2^{2^n} + 1$ عدد فردي، فإنه إذا كان يمكن كتابته كمجموع عددين أوليين فلابد أن يكون أحد هذين العددين العدد الأولي 2 ومن ثم فالعدد الآخر هو $F_n - 2$. لكن

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

عدد مؤلَّف لأن $2^{2^{n-1}} - 1 \geq 3$ إذا كان $n \geq 2$. إذاً عدد فيرما F_n لا يمكن أن يُكتَب كمجموع عددين أوليين عندما يكون $n \geq 2$.

125. بما أن $2^{2^n} \equiv -1 \bmod F_n$، فإنه برفع الطرفين إلى الأُس $2^{2^n - n}$ نحصل على $2^{F_n - 1} \equiv 1 \bmod F_n$، أي أن F_n عدد شبه أولي للأساس 2.

126. نُريد أن نُثبِت أن التطابق $2^{2^x} + 1 \equiv 0 \bmod p$ قابل للحل لعدد لانهائي من الأعداد الأولية p. سوف نقوم بإنشاء عدد لانهائي من الأعداد الأولية التي تُحقِق ذلك. من مثال 35 لدينا $(F_n, F_m) = 1$ لأي عددين صحيحين موجبين $n \neq m$.

ليكن p_1 عدداً أولياً يقسم F_1.

ليكن p_2 عدداً أولياً يقسم F_2. بما أن $(F_1, F_2) = 1$ فإن $p_2 \neq p_1$.

ليكن p_3 عدداً أولياً يقسم F_3. بما أن $(F_3, F_2) = (F_3, F_1) = 1$ فإن $p_3 \neq p_2$ و $p_3 \neq p_1$.

وهكذا إذا كان p_k عدداً أولياً يقسم F_k فإن $p_k \neq p_{k-1}, \cdots, p_2, p_1$ لأن $(F_k, F_j) = 1$ للقيم $j = 1, 2, \cdots, k-1$.

هذا يُعطينا مُتتالية لانهائية من الأعداد الأولية المختلفة $\{p_n\}_{n=1}^{+\infty}$ التي تُحقِق $p_n \mid F_n$ لجميع القيم $n \geq 1$. هذا يقتضي أنه لأي $n \geq 1$ فإن التطابق $2^{2^x} + 1 \equiv 0 \bmod p_n$ يوجد له حل هو $x = n$، وبهذا يتم الإثبات.

127. إذا كان $M_n = 2^n - 1$، $n > 2$، عدداً أولياً، فإن n عدد أولي فردي. هذا يقتضي أن

$$M_n = 2^n - 1 \equiv (-1)^n - 1 \equiv -2 \bmod 3$$

ومنه تستنتج أن $3 | M_n + 2$. لكن عندما تكون $n > 2$، فإن $M_n + 2 \geq 9$. هذا يقتضي أن $M_n + 2$ عدد مؤلَّف.

128. المطلوب هو إثبات أن $2^{M_n - 1} \equiv 1 \bmod M_n$. بما أن n عدد شبه أولي للأساس 2 فإن $2^{n-1} \equiv 1 \bmod n$. هذا يقتضي أن $2^{n-1} - 1 = nk$ حيث k عدد صحيح موجب. لاحظ ما يأتي:

$$2^{M_n - 1} - 1 = 2^{2^n - 2} - 1 = 2^{2nk} - 1 = (2^n)^{2k} - 1$$

حيث إنَّ $M_n = 2^n - 1 | (2^n)^{2k} - 1$، إذاً $M_n | 2^{M_n - 1} - 1$، أي أن $2^{M_n - 1} \equiv 1 \bmod M_n$.

129. إذا كان p عدداً أولياً فإنه إما M_p عدد أولي أو عدد شبه أولي للأساس 2 (مثال 39). في كلتا الحالتين نحصل على التطابق

$$2^{M_p - 1} \equiv 1 \bmod M_p$$

بضرب التطابق بالعدد 4 ومن ثم إضافة العدد 1 للطرفين نحصل على التطابق

$$F_p \equiv 5 \bmod M_p$$

لكن حيث إنَّ $F_1 = 5$ و $(F_1, F_p) = 1$، إذاً $(F_p, M_p) = 1$.

130. نُريد إيجاد عددين صحيحين $n \geq 0$ و $k > 1$ يُحققان المعادلة $F_n = M_k$، أي

$$2^{2^n}+1=2^k-1$$

لِنفرض أولاً أن $n \geq 1$. بما أن $2^{2^n}+1 \equiv (-1)^{2^n}+1 \equiv 2 \bmod 3$ و $2^k-1 \equiv (-1)^k-1 \equiv 0,1 \bmod 3$، اعتماداً على كون k زوجي أو فردي، إذاً $2^{2^n}+1 \not\equiv 2^k-1 \bmod 3$ ومن ثم فإن $2^{2^n}+1 \neq 2^k-1$ عندما $n \geq 1$. بقِيَ أن نختبر القيمة $n=0$. في هذه الحالة نجد أن $2^{2^0}+1=2^k-1$ ومن ثم $k=2$، أي أن $(n,k)=(0,2)$ هو الحل الوحيد للمعادلة أعلاه. هذا يقتضي أن العدد الذي هو معاً عدد فيرما و عدد مِرسان هو العدد $3=2^2-1=2^{2^0}+1$ فقط.

131. من مُعطى السؤال نجد أن $a^h \equiv 1 \bmod p$، أي أن

$$p \mid a^h-1=(a-1)(a^{h-1}+a^{h-2}+\cdots+a+1)$$

هذا بدوره يقتضي أنه إما $p \mid a-1$ أو $p \mid a^{h-1}+a^{h-2}+\cdots+a+1$. لكن بما أن $h>1$ فإن $p \nmid a-1$. هذا يقتضي أن $p \mid a^{h-1}+a^{h-2}+\cdots+a+1$، وهو المطلوب.

132. لِنكتب $\operatorname{ord}_{F_n}(2)=h$. بما أن $2^{2^{n+1}}-1=(2^{2^n}+1)(2^{2^n}-1)=F_n(2^{2^n}-1)$ فإن $2^{2^{n+1}} \equiv 1 \bmod F_n$. هذا يقتضي أن $h \mid 2^{n+1}$ ومن ثم $h=2^j$ حيث j عدد صحيح يُحقق $0 \leq j \leq n+1$. لِنفرض أن $j \leq n$. هذا يعني أن $2^{2^j} \equiv 1 \bmod F_n$ ومن ثم $F_n \mid 2^{2^j}-1=F_j-2$، وهذا مستحيل لأن $F_j-2 \leq F_n-2<F_n$. نستنتج من ذلك أن $j=n+1$، أي أن $h=2^{n+1}$ و $\operatorname{ord}_{F_n}(2)=2^{n+1}$.

133. لِنضع $t=[h,k]$. نُريد أن نُثبِت أن $\operatorname{ord}_{[m,n]}(a)=t$. بما أن $a^t \equiv 1 \bmod [m,n]$ فإننا نحصل على التطابقين

$$a^t \equiv 1 \bmod m;\ \ a^t \equiv 1 \bmod n$$

وهـذا بـدوره يقتـضي أن $\mathrm{ord}_m(a)=h \mid t$ و $\mathrm{ord}_n(a)=k \mid t$.
نستنتج من ذلك أن $[h,k] \mid t$.

أيضـاً بملاحظـة أن $h \mid [h,k]$ و $k \mid [h,k]$ فإننـا نحصـل عـلى التطابقين

$$\begin{cases} a^h \equiv 1 \bmod m \Rightarrow a^{[h,k]} \equiv 1 \bmod m \\ a^k \equiv 1 \bmod n \Rightarrow a^{[h,k]} \equiv 1 \bmod n \end{cases}$$

هذا يقتضي أن $a^{[h,k]} \equiv 1 \bmod [m,n]$ ومن ثم $t \mid [h,k]$. الآن حيث إنَّ t و $[h,k]$ عـددان صـحيحان موجبـان و $[h,k] \mid t$ و $t \mid [h,k]$ فإننـا نحصل على المساواة $t=[h,k]$، وهو المطلوب.

134. العدد المطلوب هو 2. هـذا يتضـح مباشرة مـن ملاحظـة أن $2^n \equiv 1 \bmod 2^n-1$ و $2^m \not\equiv 1 \bmod 2^n-1$ لأي عدد موجب m أقـلِّ من n وذلك لأن $2^n-1 \nmid 2^m-1$ عندما $m<n$.

135. لِنفـرض أن $q \mid a^p-1$، أي أن $a^p \equiv 1 \bmod q$. لِنضـع $\mathrm{ord}_q(a)=h$. هـذا يقتـضي أن $h \mid p$ ومنـه نسـتنتج أنـه إمـا $h=1$ أو $h=p$. إذا كان $h=1$ فإن $a \equiv 1 \bmod q$ ومن ثم $q \mid a-1$. أما إذا كان $h=p$ فإن $p=h \mid \phi(q)=q-1$ ومن ثم $q-1=pl$، حيث l عـدد صحيح موجب. بـما أن p و q عـددان فرديـان فلابـد أن يكـون l عـدداً زوجيـاً، $l=2k$، حيـث k عـدد صـحيح موجـب. هـذا يقتـضي أن $q=2kp+1$.

136. بـما أن g جـذر بـدائي قيـاس p فـإن الأعـداد

$g, g^2, g^3, \cdots, g^{p-1}$ تُمثل نظام رواسب مُختزَل قياس p (نظرية 26).
أيضاً الأعداد $1,2,3,\cdots,p-1$ تُمثل نظام رواسب مُختزَل قياس p. هذا يقتضي أن كل عدد من الأعداد $g, g^2, g^3, \cdots, g^{p-1}$ يُطابق قياس p عدداً واحداً فقط من الأعداد $1,2,3,\cdots,p-1$. نستنتج من ذلك أن

$$g + g^2 + g^3 + \cdots + g^{p-1} \equiv 1+2+3+\cdots+(p-1) \bmod p$$

لكن

$$1+2+3+\cdots+(p-1) = \frac{(p-1)}{2} \cdot p \equiv 0 \bmod p$$

إذاً نستنتج أن

$$g + g^2 + g^3 + \cdots + g^{p-1} \equiv 0 \bmod p$$

137. لنأخذ عدداً صحيحاً a بحيث يكون $(a,pq)=1$. سوف نقوم بإثبات أن $\text{ord}_{pq}(a) \neq \phi(pq)$. هذا سوف يُثبت أنه لا يوجد جذر بدائي قياس pq. بما أن $(a,pq)=1$ فإن $(a,p)=(a,q)=1$. باستخدام نظرية فيرما نحصل على التطابقين الآتيين:

$$a^{p-1} \equiv 1 \bmod p, \quad a^{q-1} \equiv 1 \bmod q$$

برفع التطابق الأول إلى الأُس $(q-1)/2$ والثاني إلى الأُس $(p-1)/2$ نحصل على الآتي:

$$a^{(p-1)(q-1)/2} \equiv 1 \bmod p, \quad a^{(q-1)(p-1)/2} \equiv 1 \bmod q$$

لأن $(p,q)=1$، إذاً $a^{(p-1)(q-1)/2} \equiv 1 \bmod pq$، أي $a^{\phi(pq)/2} \equiv 1 \bmod pq$. من ذلك نستنتج أن $\text{ord}_{pq}(a) \leq \phi(pq)/2 < \phi(pq)$ ومن ثم $\text{ord}_{pq}(a) \neq \phi(pq)$.

138. بما أن 2 جذر بدائي قياس 13 فإن الأعداد $2,2^2,2^3,\cdots,2^{12}$ تُمثل نظام رواسب مُختزَل قياس 13. إذا كان $x^9 \equiv 12 \bmod 13$ فإن $(x^9,13)=(12,13)=1$ ومن ثم $(x,13)=1$. هذا يقتضي أن $x\equiv 2^i \bmod 13$، حيث i عدد صحيح يُحقق $1\le i\le 12$. أيضاً نلاحظ أن $12\equiv 2^6 \bmod 13$. الآن يمكن أن نكتب التطابق $x^9\equiv 12 \bmod 13$ على الشكل $2^{9i}\equiv 2^6 \bmod 13$. هذا يقتضي أن $9i\equiv 6 \bmod 12$. حلول هذا التطابق الخطي هي $i\equiv 2,6,10 \bmod 12$ ومن ثم فإن حلول التطابق $x^9\equiv 12 \bmod 13$ هي $x\equiv 2^2,2^6,2^{10}\equiv 4,12,10 \bmod 13$.

139. نفرض أولاً أن $p-1\,|\,n$. هذا يقتضي أن $n=(p-1)k$، حيث k عدد صحيح موجب. باستخدام نظرية فيرما نجد أن $i^{p-1}\equiv 1 \bmod p$ لجميع الأعداد $1\le i\le p-1$. برفع طرفي التطابق إلى الأُس k نحصل على التطابق $i^n\equiv 1 \bmod p$ لجميع الأعداد $1\le i\le p-1$. نستنتج من ذلك أن

$$\begin{aligned} S_n(p) &= 1^n+2^n+\cdots+(p-1)^n \\ &\equiv 1+1+\cdots+1=p-1\equiv -1 \bmod p \end{aligned}$$

نفرض ثانياً أن $p-1\nmid n$. نأخذ جذراً بدائياً g قياس p. الأعداد $1,g,g^2,\cdots,g^{p-2}$ تُمثل نظام رواسب مُختَزَل قياس p (نظرية 26). بملاحظة أن الأعداد $1,2,3,\cdots p-1$ تُمثِل نظام رواسب مُختَزَل قياس p نستنتج أن

$$\begin{aligned} S_n(p) &= 1^n+2^n+3^n+\cdots+(p-1)^n \\ &\equiv 1+g^n+g^{2n}+\cdots+g^{(p-2)n} \bmod p \end{aligned}$$

حيث إنَّ $p-1\nmid n$ فإن $g^n-1\not\equiv 0 \bmod p$ (لو كان $g^n\equiv 1 \bmod p$ فإن $\operatorname{ord}_p(g)=p-1\,|\,n$ وهذا يُخالِف الفرض

$n \nmid p-1$.) بِضرب طرفي التطابق السابق بالعدد $g^n - 1$ نحصل على التطابق

$$\begin{aligned}(g^n - 1)S_n(p) &\equiv g^{(p-1)n} - 1\\ &\equiv 0 \bmod p\end{aligned}$$

بما أن $p \mid (g^n - 1)S_n(p)$ و $p \nmid g^n - 1$ فإن $p \mid S_n(p)$، أي أن $S_n(p) \equiv 0 \bmod p$.

140. لإثبات أن $N = pq$، حيث إنَّ $p < q$ عددان أوليان فرديان، ليس عدداً كارمايكيلياً، نقوم بإيجاد عدد صحيح a يُحقِق $(a,N) = 1$ و $a^{N-1} \not\equiv 1 \bmod N$.

ليكن g_1 جذراً بدائياً قياس p و g_2 جذراً بدائياً قياس q، أي أن $\mathrm{ord}_p(g_1) = p-1$ و $\mathrm{ord}_q(g_2) = q-1$. باستخدام نظرية الباقي الصينية يوجد عدد صحيح a يُحقِق التطابقين

$$a \equiv g_1 \bmod p, \quad a \equiv g_2 \bmod q$$

لِنضع $h = \mathrm{ord}_N(a)$. إذاً $a^h \equiv 1 \bmod N$ و منه $(a,N) = 1$. هذا يقتضي أن $a^h \equiv 1 \bmod q$. بما أن $a \equiv g_2 \bmod q$ فإننا نستنتج أن $g_2^h \equiv 1 \bmod q$ ومن ثم $q-1 \mid h$.

الآن لِنفرض أن $a^{N-1} \equiv 1 \bmod N$. هذا يقتضي أن $h \mid N-1 = pq-1 = q(p-1)+(q-1)$. بما أن $q-1 \mid h$ فإن $q-1 \mid q(p-1)+(q-1)$ ومن ثم $q-1 \mid q(p-1)$. بما أن $(q-1,q) = 1$ فإننا نستنتج أن $q-1 \mid p-1$ ومن ثم $q-1 \leq p-1$ وهذا مستحيل لأن $p < q$. إذاً $a^{N-1} \not\equiv 1 \bmod N$ ومن ثم فإن $N = pq$ ليس عدداً كارمايكيلياً.

141. لِنضع $\operatorname{ord}_{p^2}(a)=t$. ندرس حالتين فيما يتعلق بقيمة $\operatorname{ord}_p(a)=h$.

الحالة الأولى: $h>1$. حيث إنَّ $\operatorname{ord}_p(a)=h$ فإن $a^h \equiv 1 \bmod p$. هذا يقتضي أن $a^h=1+kp$ حيث k عدد صحيح. باستخدام نظرية ذات الحدين نستنتج أن

$$a^{hp}=(1+kp)^p \equiv 1 \bmod p^2$$

ومن ثم $t \mid hp$. هذا يؤدي إلى الاحتمالات التالية لقيم t:

$$t=1,h,p,hp,r,rp \quad (r \mid h, 1<r<h)$$

إذا كان $t=1$ فإن $a^1 \equiv 1 \bmod p^2$ يقتضي أن $a \equiv 1 \bmod p$ وهذا مستحيل لأن $h>1$. إذا كان $t=p$ فإن $a^p \equiv 1 \bmod p^2$ يقتضي أن $a^p \equiv 1 \bmod p$ ومن ثم $a \equiv 1 \bmod p$ وهذا مستحيل لأن $h>1$. إذا كان $t=r$ فإن $a^r \equiv 1 \bmod p^2$ يقتضي أن $a^r \equiv 1 \bmod p$ وهذا مستحيل لأن $r<h$. إذا كان $t=rp$ فإن $a^{rp} \equiv 1 \bmod p^2$ يقتضي أن $a^{rp} \equiv 1 \bmod p$ ومن ثم $a^r \equiv 1 \bmod p$ (لأن $a^p \equiv a \bmod p$) وهذا مستحيل لأن $r<h$. نستنتج من ذلك أن $t=h$ أو $t=hp$.

الحالة الثانية: $h=1$. حيث إنَّ $\operatorname{ord}_p(a)=1$ فإن $a \equiv 1 \bmod p$. هذا يقتضي أن $a=1+kp$ حيث k عدد صحيح. عند كتابة $k=l+sp$ حيث $0 \le l \le p-1$ سوف نحصل على $a=1+lp+sp^2 \equiv 1+lp \bmod p^2$ ومنه (باستخدام نظرية ذات الحدين)

$$a^p \equiv (1+lp)^p \equiv 1 \bmod p^2$$

هذا يقتضي أن $t \mid p$ ومن ثم $t=1$ أو $t=p$.

إذاً في كلتا الحالتين h $\operatorname{ord}_{p^2}(a)=t=h$ أو $\operatorname{ord}_{p^2}(a)=t=hp$.

142. لاحظ أولاً أنه من مُعطَى السؤال نستنتج أن $(a,m)=1$ وأن التطابق $x^2\equiv a \bmod m$ قابل للحل، أي أنه يوجد عدد صحيح x_0 بحيث $x_0^2\equiv a \bmod m$. بما أن $(a,m)=1$، فإن $(x_0,m)=1$. باستخدام نظرية أويلر، نحصل على $x_0^{\phi(m)}\equiv 1 \bmod m$. بما أن $x_0^2\equiv a \bmod m$، فإن

$$a^{\phi(m)/2}\equiv x_0^{\phi(m)}\equiv 1 \bmod m$$

وهو المطلوب.

143. إذا كان $p\equiv 3 \bmod 8$ فإن $\left(\frac{2}{p}\right)=-1$. حيث إنَّ $\left(\frac{2}{p}\right)\equiv 2^{(p-1)/2} \bmod p$ فإن $2^{(p-1)/2}\equiv -1 \bmod p$، أي أن $p \mid 2^{(p-1)/2}+1$.

144. من العلاقة $\left(\frac{5}{p}\right)\left(\frac{-1}{p}\right)=\left(\frac{-5}{p}\right)=1$ نستنتج أنه إما $\left(\frac{5}{p}\right)=1$ و $\left(\frac{-1}{p}\right)=1$ أو $\left(\frac{5}{p}\right)=-1$ و $\left(\frac{-1}{p}\right)=-1$. في الحالة الأُولى p يجب أن يُحقق $p\equiv 1,4 \bmod 5$ و $p\equiv 1 \bmod 4$، وفي الحالة الثانية p يجب أن يُحقق $p\equiv 2,3 \bmod 5$ و $p\equiv 3 \bmod 5$ (نظرية 29، فقرة 5 و مثال 48). باستخدام نظرية الباقي الصينية نجد أن $\left(\frac{-5}{p}\right)=1$ إذا وفقط إذا كان $p\equiv 1,3,7,9 \bmod 20$.

145. باستخدام قانون جاوس للمقلوبية نجد أن

$$\left(\frac{p}{q}\right)=\left(\frac{p}{6p+1}\right)=(-1)^{\frac{p-1}{2}\frac{6p}{2}}\left(\frac{6p+1}{p}\right)=(-1)^{\frac{p-1}{2}}\left(\frac{1}{p}\right)=(-1)^{\frac{p-1}{2}}$$

146. لِنضـــــع $p=4^n+1$. نلاحـــــظ أن $p\equiv 1 \bmod 4$ و $p\equiv 1^n+1\equiv 2 \bmod 3$. الإثبات ينتج من الحسابات الآتية:

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

147. إذا كـان $p=4n+1$ وكـان $q\mid n$، فـإن $p\equiv 1 \bmod q$.
باستخدام قانون جاوس للمقلوبية نستنتج أن

$$\left(\frac{q}{p}\right)=\left(\frac{p}{q}\right)=\left(\frac{1}{q}\right)=1$$

148. لِنفرض أن q عدد مؤلَّف، أي أن $q=ab$ حيث $1<a<b<q$ ($a\neq b$ وإلا سوف يكون $q=a^2$ راسباً تربيعياً.) الآن بما أن

$$-1=\left(\frac{q}{p}\right)=\left(\frac{ab}{p}\right)=\left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$$

فإنه إمـا $\left(\frac{a}{p}\right)=-1$ أو $\left(\frac{b}{p}\right)=-1$، أي أن a أو b سيكون راسباً غير تربيعي قياس p وكلاهما أقل من q، وهذا يُناقِض كَون q هو أصغر راسب غير تربيعي موجب قياس p. هذا التناقض يُثبت أن q عدد أولي.

149. حيث إنَّ $\left(\frac{n}{p}\right)=1$ فإن $n^{(p-1)/2}\equiv 1 \bmod p$. بملاحظة أن

$$(n^{k+1})^2=n\cdot n^{2k+1}=n\cdot n^{(p-1)/2}\equiv n\cdot 1\equiv n \bmod p$$

نستنتج أن $x\equiv n^{k+1} \bmod p$ هو حلٌّ للتطابق $x^2\equiv n \bmod p$.

150. إذا كان $p>3$ عدداً أولياً بحيث $p \mid n^2-6n+90$ لعدد صحيح n فإن $n^2-6n+90 \equiv 0 \bmod p$، أو $(n-3)^2 \equiv -81 \bmod p$. بما أن $(p,81)=1$ فإن $(p,(n-3)^2)=1$.
هذا يقتضي أن

$$1=\left(\frac{(n-3)^2}{p}\right)=\left(\frac{-81}{p}\right)=\left(\frac{-1}{p}\right)\left(\frac{81}{p}\right)=\left(\frac{-1}{p}\right)$$

ومن ثم $p \equiv 1 \bmod 4$ (ملحوظة 1 لنظرية 29) وهو المطلوب.

151. إذا كان $\left(\frac{3}{p}\right)=1$ أو $\left(\frac{5}{p}\right)=1$، فإن $x^2-3 \equiv 0 \bmod p$ أو $x^2-5 \equiv 0 \bmod p$ قابل للحل. هذا بدوره يقتضي أن التطابق $(x^2-3)(x^2-5)(x^2-15) \equiv 0 \bmod p$ قابل للحل.

أما إذا كان $\left(\frac{3}{p}\right)=-1$ و $\left(\frac{5}{p}\right)=-1$، فإن $1=\left(\frac{5}{p}\right)\left(\frac{3}{p}\right)=\left(\frac{15}{p}\right)$ ومن ثم فإن التطابق $x^2-15 \equiv 0 \bmod p$ قابل للحل. هذا أيضاً يقتضي أن التطابق $(x^2-3)(x^2-5)(x^2-15) \equiv 0 \bmod p$ قابل للحل.

152. نُثبت أنه لأي عدد صحيح $m \geq 2$ يوجد عدد أولي $p \equiv 4 \bmod 5$ أكبر من m. هذا سوف يُثبت وجود عدد غير منتهٍ من الأعداد الأولية ذات الشكل العام $5n+4$.

ليكن $m \geq 2$ عدداً صحيحاً. لِنضع $A=5(m!)^2-1$. إذا كان $p>2$ عدداً أولياً بحيث إنَّ $p \mid A$ فإن $p \neq 5$ و $p>m$ (وإلا سوف نحصل على $p \mid 1$ وهذا تناقض واضح.) نستنتج من ذلك أن

$(p,5(m!)^2)=1$. أيضاً بما أن $p\mid A$ فإن $5(m!)^2\equiv 1 \bmod p$. هذا يقتضي أن

$$1=\left(\frac{1}{p}\right)=\left(\frac{5(m!)^2}{p}\right)=\left(\frac{5}{p}\right)\left(\frac{(m!)^2}{p}\right)=\left(\frac{5}{p}\right)$$

ومن ثم $p\equiv 1,\ 4 \bmod 5$ (مثال 48). بملاحظة أن $A\equiv 4 \bmod 5$ نستنتج أن القواسم الأولية للعدد A لا يمكن أن تكون جميعها على الشكل $5k+1$ (وإلا فإن A سوف يأخذ نفس الشكل، وهذا تناقض). إذاً لابد أن يكون أحد القواسم الأولية للعدد A يُحقق $p\equiv 4 \bmod 5$ وهو ما نُريده. بهذا يتم الإثبات.

153. نفرض أنه يوجد عدد منتهٍ من الأعداد الأولية ذات الشكل العام $8n+7$. لِتكن هذه الأعداد الأولية $p_1,p_2,\cdots,p_r$. نقوم بإثبات وجود عدد أولي p صورته العامة $8n+7$ مختلف عن $p_1,p_2,\cdots,p_r$. هذا التناقض يقتضي وجود عدد غير منتهٍ من الأعداد الأولية ذات الشكل العام $8n+7$.

لِنعرف العدد $A=(4p_1p_2\cdots p_r)^2-2$. إذاً A عدد زوجي و $A\equiv -2 \bmod 8$. في الحقيقة $2\parallel A$. ليكن p عدداً أولياً فردياً بحيث $p\mid A$. هذا يقتضي أن $p\neq p_i$ لجميع القيم $1\le i\le r$، وإلا سوف نحصل على $p\mid 2$ وهذا مستحيل. من ذلك نستنتج أن $(p,4p_1p_2\cdots p_r)=1$. أيضاً بما أن $p\mid A$ فإن $(4p_1p_2\cdots p_r)^2\equiv 2 \bmod p$. هذا يقتضي أن

$$1=\left(\frac{(4p_1p_2\cdots p_r)^2}{p}\right)=\left(\frac{2}{p}\right)$$

ومن ثم $p\equiv 1,\ 7 \bmod 8$. إذا كانت $8n+1$ هي الصورة العامة لجميع

الأعداد الأولية الفردية التي تقسم A فإن $A=2(8k+1)\equiv 2 \bmod 8$ وهذا تناقض واضح. إذاً لابد أن يوجد عدد أولي $p\equiv 7 \bmod 8$ يقسم A . بهذا يتم الإثبات.

154. نفرض أولاً أن $2^p \equiv 1 \bmod 2p+1$ وأن $2p+1=\prod_{i=1}^{r} p_i^{\alpha_i}$. هذا يقتضي أن $\text{ord}_{2p+1}2 \mid p$ ومن ثم إما $\text{ord}_{2p+1}2=1$ أو $\text{ord}_{2p+1}2=p$. لكن بما أن $2\neq 1 \bmod 2p+1$ فإن $\text{ord}_{2p+1}2=p$. أيضاً من التطابق $2^p\equiv 1 \bmod 2p+1$ نستنتج أن $p=\text{ord}_{2p+1}2\mid \phi(2p+1)$، أي أن

$$p \mid \prod_{i=1}^{r} p_i^{\alpha_i-1}(p_i-1)$$

هذا يقتضي أنه يوجد i، حيث $1\le i\le r$، يُحقق $p\mid p_i-1$.

لنكتب $2p+1=p_i n$ حيث $n\ge 1$ عدد صحيح. نلاحظ أن $n\neq 2$ وإلا سوف يصبح لدينا $2\mid 1$ وهذا مستحيل. إذا كان $n>2$ فإن $2p+1=p_i n>2p_i$ يقتضي أن $p>p_i-\frac{1}{2}>p_i-1$ ومن ثم $p\nmid p_i-1$، وهذا يُناقض ما أثبتناه أعلاه. إذاً نستنتج أنه لابد أن يكون $n=1$ ومن ثم $2p+1=p_i$، أي أن $2p+1$ عدد أولي.

أما العكس، فإذا كان $2p+1$ عدداً أولياً و $p=4k+3$، فإن $2p+1=8k+7\equiv 7 \bmod 8$. هذا يقتضي أن $\left(\frac{2}{2p+1}\right)=1$ ومن ثم $2^{\frac{2p+1-1}{2}}\equiv 1 \bmod 2p+1$، أي أن $2^p\equiv 1 \bmod 2p+1$، وهو المطلوب.

155. حيث إنَّ g جذر بدائي قياس p، فإن $g^{p-1}\equiv 1 \bmod p$. هذا يقتضي أن

$$g^{p-1}-1=(g^{(p-1)/2}-1)(g^{(p-1)/2}+1)\equiv 0 \bmod p$$

ومن ثم إما $g^{(p-1)/2}\equiv -1 \bmod p$ أو $g^{(p-1)/2}\equiv 1 \bmod p$. الاحتمال الثاني غير ممكن لأن g جذر بدائي قياس p. لذا نحصل على $g^{(p-1)/2}\equiv -1 \bmod p$. الآن حيث إنَّ $g^{(p-1)/2}\equiv \left(\frac{g}{p}\right) \bmod p$، إذاً $\left(\frac{g}{p}\right)\equiv -1 \bmod p$. و بسبب أن $\left(\frac{g}{p}\right)=\pm 1$ و p عدد أولي فردي، نستنتج أن $\left(\frac{g}{p}\right)=-1$، أي أن g راسب غير تربيعي قياس p.

156. لنرمز لعدد عناصر المجموعة A بالرمز $|A|$. لتكن S هي مجموعة الرواسب غير التربيعية قياس p و T هي مجموعة الجذور البدائية قياس p. السؤال السابق يقتضي أن $T\subseteq S$. نعرف أيضاً أن $|S|=\frac{p-1}{2}$ و $|T|=\phi(p-1)$.

إذا كان عكس السؤال السابق صحيح فإن هذا يقتضي أن $S\subseteq T$ ومن ثم $S=T$. هذا يعني أن $\phi(p-1)=\frac{p-1}{2}$، وهذا صحيح إذا و فقط إذا كان $p-1=2^k$، أي $p=2^k+1$، حيث k عدد صحيح موجب. (مثال 21)

إذا كان $p=2^k+1$ فإن $|S|=\frac{p-1}{2}=2^{k-1}$ و $|T|=\phi(p-1)=\phi(2^k)=2^{k-1}$. هذا يقتضي أن $|S|=|T|$. بما أن $T\subseteq S$ إذاً لابد أن يكون $S=T$، أي أن كل راسب غير تربيعي قياس p هو جذر بدائي قياس p.

157. ليكن عدد فيرما $F_n=2^{2^n}+1$، $n\geq 1$، عدداً أولياً. نلاحظ أولاً أن $F_n\equiv 1 \bmod 4$ و $F_n\equiv 2 \bmod 3$. باستخدام قانون جاوس

للمقلوبية نحصل على

$$\left(\frac{3}{F_n}\right)=\left(\frac{F_n}{3}\right)=\left(\frac{2}{3}\right)=-1$$

أي أن 3 راسب غير تربيعي قياس F_n. باستخدام السؤال السابق نستنتج أن 3 جذر بدائي قياس F_n.

158. لاحظ أن $p=2q+1$. نلاحظ أيضاً ما يأتي:

- أي جذر بدائي قياس p هو راسب غير تربيعي قياس p (سؤال رقم 155)
- العدد 2 هو راسب غير تربيعي قياس p لأن $p\equiv 3 \bmod 8$ (ملحوظة 2 لنظرية 29)
- يوجد $q=\dfrac{p-1}{2}$ راسب غير تربيعي قياس p (نظرية 28) و $\phi(p-1)=q-1$ جذر بدائي قياس p (نظرية 27)
- $p-1$ راسب غير تربيعي قياس p (لأن $p-1\equiv -1 \bmod p$ و $p\equiv 3 \bmod 4$) و ليس جذراً بدائياً قياس p (لأن رُتبتُهُ 2 وليس $p-1$)

نستنتج من هذه الملحوظات أن كل الرواسب غير التربيعية قياس p (باستثناء $p-1$) هي جذور بدائية قياس p. فحيث إنَّ 2 راسب غير تربيعي قياس p فإن 2 جذر بدائي قياس p.

159. بتقسيم n على m نحصل على

$$n=mq+r,\quad 0\le r<m$$

من ذلك نستنتج أن

$$\left[\!\left[\frac{n}{m}\right]\!\right]=\left[\!\left[q+\frac{r}{m}\right]\!\right]=q+\left[\!\left[\frac{r}{m}\right]\!\right]=q$$

و أيضاً

$$\left[\!\left[\frac{n-1}{m}\right]\!\right]=\left[\!\left[q+\frac{r-1}{m}\right]\!\right]=q+\left[\!\left[\frac{r-1}{m}\right]\!\right]=\begin{cases} q, & 1\le r<m \\ q-1, & r=0 \end{cases}$$

هذا يقتضي أن

$$\left[\!\left[\frac{n}{m}\right]\!\right]-\left[\!\left[\frac{n-1}{m}\right]\!\right]=\begin{cases} 1, & m\mid n \\ 0, & m\nmid n \end{cases}$$

160. باستخدام خواص دالة الصحيح $[\![x]\!]$ نجد أن

$$nx-1<[\![nx]\!]\le nx$$

و $n(x-1)<n[\![x]\!]\le nx$، أو

$$-nx\le -n[\![x]\!]<-n(x-1)$$

بجمع المتباينات أعلاه نحصل على

$$-1<[\![nx]\!]-n[\![x]\!]<n$$

حيث إنَّ $[\![nx]\!]-n[\![x]\!]$ عدد صحيح، إذاً $0\le[\![nx]\!]-n[\![x]\!]\le n-1$.

161. بملاحظة أن

$$3^{2n}\le 3^{2n}+3^n+3<3^{2n}+2\times 3^n+1=(3^n+1)^2$$

نجد أن

$$3^n \le \sqrt{3^{2n}+3^n+3} < 3^n+1$$

هذا يقتضي أن $\left[\!\left[\sqrt{3^{2n}+3^n+3}\right]\!\right] = 3^n$.

162. إذا كان $i=1$ فإن $\left[\!\left[\frac{[\![p/1]\!]}{p/1}\right]\!\right]=1$. الآن لنفرض أن $1<i\le p-1$. بما أن $x-1<[\![x]\!]\le x$، حيث $[\![x]\!]=x$ إذا وفقط إذا كان x عدداً صحيحاً، و p/i ليس عدداً صحيحاً، إذاً

$$\frac{p}{i}-1<\left[\!\left[\frac{p}{i}\right]\!\right]<\frac{p}{i}$$

بالتقسيم على p/i نحصل على

$$0<1-\frac{i}{p}<\frac{[\![p/i]\!]}{p/i}<1$$

ومن ثم $\left[\!\left[\frac{[\![p/i]\!]}{p/i}\right]\!\right]=0$. هذا يقتضي أن $\sum_{i=1}^{p-1}\left[\!\left[\frac{[\![p/i]\!]}{p/i}\right]\!\right]=1$.

163. نبدأ الحل بذكر ملحوظتين:

- $x-1<[\![x]\!]\le x$ و $[\![x]\!]=x$ إذا و فقط إذا كان x عدداً صحيحاً.
- بواسطة نظرية ويلسون، $n+1 \mid n!+1$ إذا و فقط إذا كان $n+1$ عدداً أولياً.

لاحظ أن

$$\frac{n!+1}{n+1}-1<\left[\!\left[\frac{n!+1}{n+1}\right]\!\right]\le\frac{n!+1}{n+1}$$

حيث إنَّ المساواة تتحقق إذا و فقط إذا كان $n+1$ عدداً أولياً. بضرب الحدود بالمقدار $n+1$، نحصل على

$$n!-n<\left[\!\left[\frac{n!+1}{n+1}\right]\!\right](n+1)\le n!+1$$

بطرح $n!-n$ من جميع الحدود ومن ثم التقسيم على $n+1$، نحصل على

$$0<\left[\!\left[\frac{n!+1}{n+1}\right]\!\right]-\left(\frac{n!-n}{n+1}\right)\le 1$$

حيث إنَّ المساواة تتحقق إذا وفقط إذا كان $n+1$ عدداً أولياً. لنضع

$$A(n)=\left[\!\left[\frac{n!+1}{n+1}\right]\!\right]-\left(\frac{n!-n}{n+1}\right)$$

إذاً $[\![A(n)]\!]=1$ إذا كان $n+1$ عدداً أولياً و $[\![A(n)]\!]=0$ إذا كان $n+1$ عدداً غير أولي. بما أن

$$f(n)=(n-1)\cdot[\![A(n)]\!]+2$$

إذاً $f(n)=n+1$ إذا كان $n+1$ عدداً أولياً و $f(n)=2$ إذا كان $n+1$ عدداً غير أولي، أي أنه في جميع الحالات $f(n)$ عدد أولي.

164. أي عدد حقيقي $\alpha>0$ يقع بين قوتين لعددين صحيحين متتاليين:

$$m^k\le\alpha<(m+1)^k$$

حيث $m\ge 0$ عدد صحيح. بما أن $0\le\alpha-[\![\alpha]\!]<1$ و $(m+1)^k-m^k\ge 1$، فإن

$$m^k\le[\![\alpha]\!]\le\alpha<(m+1)^k$$

هذا يقتضي أن $m \le \sqrt[k]{[\![\alpha]\!]} \le \sqrt[k]{\alpha} < m+1$ ومن ثم $[\![\sqrt[k]{\alpha}]\!] = m = [\![\sqrt[k]{[\![\alpha]\!]}]\!]$.

165. لاحظ أولاً أن $[\![\alpha]\!] = 0$ ومن ثم فالصفر ينتمي إلى المجموعة المعطاة. ليكن n عدداً صحيحاً موجباً. العدد n يقع بين مضاعفين متتاليين للعدد α:

$$(m-1)\alpha < n \le m\alpha$$

حيث $m > 1$ عدد صحيح. بما أن $0 < \alpha < 1$، فإن $-\alpha > -1$. هذا يقتضي أن $m\alpha - 1 < n \le m\alpha$، أو $n \le m\alpha < n+1$. نستنتج من ذلك أن $[\![m\alpha]\!] = n$.

166. ليكن k أكبر عدد صحيح يُحقق $5^k \le n < 5^{k+1}$. إذاً

$$e_5 = \sum_{i=1}^{+\infty} \left[\!\!\left[\frac{n}{5^i}\right]\!\!\right] = \sum_{i=1}^{k} \left[\!\!\left[\frac{n}{5^i}\right]\!\!\right]$$

حيث إنَّ $n \ge 5^k > 4^k = 2^{2k}$ و $[\![n/2^i]\!] \ge [\![n/5^i]\!]$ (لأن $n/2^i \ge n/5^i$ لأي $i \ge 1$) نستنتج أن

$$e_2 = \sum_{i=1}^{+\infty} [\![n/2^i]\!] \ge \sum_{i=1}^{2k} [\![n/2^i]\!] > \sum_{i=1}^{k} [\![n/2^i]\!] \ge \sum_{i=1}^{k} [\![n/5^i]\!] = e_5$$

أي أن $e_2 > e_5$.

167. إذا كان $(n,12) = 1$ فإن $(n,2) = (n,3) = 1$. عدد الأعداد الأقل من أو تساوي 1000 والتي تقبل القسمة على 2 تساوي $\left[\!\!\left[\frac{1000}{2}\right]\!\!\right] = 500$ والتي تقبل القسمة على 3 تساوي $\left[\!\!\left[\frac{1000}{3}\right]\!\!\right] = 333$ والتي تقبل القسمة على 2 و 3 معاً تساوي $\left[\!\!\left[\frac{1000}{6}\right]\!\!\right] = 166$. إذاً فالعدد المطلوب يساوي $1000 - 500 - 333 + 166 = 333$.

168. باستخدام نظرية ذات الحدين يمكننا أن نكتب (لقيم $n \geq 1$)

$$(3+2\sqrt{2})^n = \sum_{k=0}^{n} \binom{n}{k} 3^{n-k} (2\sqrt{2})^k = a_n + b_n\sqrt{2},$$

$$(3-2\sqrt{2})^n = \sum_{k=0}^{n} \binom{n}{k} 3^{n-k} (-2\sqrt{2})^k = a_n - b_n\sqrt{2}$$

حيث a_n و b_n أعداد صحيحة. (قيمة b_n ناتجة من الحدود التي فيها k عدد فردي.) بضرب المعادلتين السابقتين نحصل على

$$a_n^2 - 2b_n^2 = 1$$

نقوم بإجراء الحسابات التالية:

$$\left[\!\left[(3+2\sqrt{2})^n\right]\!\right] = \left[\!\left[a_n + b_n\sqrt{2}\right]\!\right] = \left[\!\left[a_n + \sqrt{2b_n^2}\right]\!\right] = \left[\!\left[a_n + \sqrt{a_n^2 - 1}\right]\!\right]$$
$$= a_n + \left[\!\left[\sqrt{a_n^2 - 1}\right]\!\right] = a_n + (a_n - 1) = 2a_n - 1$$

إذاً فالمقدار $\left[\!\left[(3+2\sqrt{2})^n\right]\!\right]$ عدد فردي.

ملحوظة: حيث إنَّ $(a_n - 1)^2 \leq a_n^2 - 1 < a_n^2$، إذاً $\left[\!\left[\sqrt{a_n^2 - 1}\right]\!\right] = a_n - 1$.

169. بما أن الأعداد $0,1,2,\cdots,m-1$ تُمثِّل نظام رواسب تام قياس m و $(a,m)=1$ فإن الأعداد

$$b\,, a+b\,, 2a+b\,, \cdots, (m-1)a+b$$

تُمثِّل أيضاً نظام رواسب تام قياس m. عند قسمة هذه الأعداد على m نحصل على

$$ai + b = \left[\!\left[\frac{ai+b}{m}\right]\!\right] m + r_i\,, \quad 0 \leq i \leq m-1$$

حيث إنَّ البواقي r_i تأخذ جميع القيم $0,1,2,\cdots,m-1$، لكن ربما بترتيب مُختلِف. بجمع المعادلات السابقة نحصل على

$$\sum_{i=0}^{m-1}(ai+b)=\sum_{i=0}^{m-1}\left[\!\left[\frac{ai+b}{m}\right]\!\right]m+\sum_{i=0}^{m-1}r_i$$

بالتبسيط وبملاحظة أن $\sum_{i=0}^{m-1}i=\sum_{i=0}^{m-1}r_i$ نحصل على الآتي:

$$a\sum_{i=0}^{m-1}i+\sum_{i=0}^{m-1}b=m\sum_{i=0}^{m-1}\left[\!\left[\frac{ai+b}{m}\right]\!\right]+\sum_{i=0}^{m-1}r_i,$$

$$(a-1)\sum_{i=0}^{m-1}i+bm=m\sum_{i=0}^{m-1}\left[\!\left[\frac{ai+b}{m}\right]\!\right],$$

$$(a-1)\cdot\frac{(m-1)m}{2}+bm=m\sum_{i=0}^{m-1}\left[\!\left[\frac{ai+b}{m}\right]\!\right]$$

بالتقسيم على m نحصل على المطلوب:

$$\sum_{i=0}^{m-1}\left[\!\left[\frac{ai+b}{m}\right]\!\right]=\frac{(a-1)(m-1)}{2}+b$$

170. نقسم الفترة $0\le x<1$ إلى n جزءاً بحيث يكون طول كل جزء $\frac{1}{n}$ ومن ثم ندرس الحالات المحتملة لقيم x:

$$\frac{i-1}{n}\le x<\frac{i}{n},\quad i=1,2,\cdots,n$$

إذا كان $i=1$ (أي أن $0\le x<\frac{1}{n}$) فإن

$$[\![x]\!]=\left[\!\left[x+\frac{1}{n}\right]\!\right]=\left[\!\left[x+\frac{2}{n}\right]\!\right]=\cdots=\left[\!\left[x+\frac{n-1}{n}\right]\!\right]=0=[\![nx]\!]$$

وإذا كان $2\le i\le n$ و $\frac{i-1}{n}\le x<\frac{i}{n}$، فإن $i-1\le nx<i$ ومن ثم $[\![nx]\!]=i-1$.

هذا يعطينا $[\![x]\!]=\left[\!\left[x+\frac{1}{n}\right]\!\right]=\left[\!\left[x+\frac{2}{n}\right]\!\right]=\cdots=\left[\!\left[x+\frac{n-i}{n}\right]\!\right]=0$

$$\left[\!\left[x+\frac{n-(i-1)}{n}\right]\!\right]=\left[\!\left[x+\frac{n-(i-2)}{n}\right]\!\right]=\cdots=\left[\!\left[x+\frac{n-1}{n}\right]\!\right]=1$$

أي أن

$$[\![x]\!]+\left[\!\left[x+\frac{1}{n}\right]\!\right]+\left[\!\left[x+\frac{2}{n}\right]\!\right]+\cdots+\left[\!\left[x+\frac{n-1}{n}\right]\!\right]=i-1=[\![nx]\!]$$

وبهذا يتم المطلوب.

171. لاحظ أولاً أنه إذا كان $k=2l+1\geq 1$ عدداً فردياً فإن

$$\left[\!\left[\frac{k}{2}\right]\!\right]=\left[\!\left[\frac{2l+1}{2}\right]\!\right]=\left[\!\left[l+\frac{1}{2}\right]\!\right]=l=\frac{k-1}{2}$$

الآن إذا كان n عدداً زوجياً فإن

$$\begin{aligned}\sum_{k=1}^{n}\left[\!\left[\frac{k}{2}\right]\!\right]&=\left[\!\left[\frac{1}{2}\right]\!\right]+\left(1+\left[\!\left[\frac{3}{2}\right]\!\right]\right)+\left(2+\left[\!\left[\frac{5}{2}\right]\!\right]\right)+\cdots+\left(\frac{n-2}{2}+\left[\!\left[\frac{n-1}{2}\right]\!\right]\right)+\frac{n}{2}\\&=2\left(1+2+\cdots+\frac{n-2}{2}\right)+\frac{n}{2}\\&=\frac{n^2}{4}=\left[\!\left[\frac{n^2}{4}\right]\!\right]\end{aligned}$$

أما إذا كان n عدداً فردياً فإن

$$\begin{aligned}\sum_{k=1}^{n}\left[\!\left[\frac{k}{2}\right]\!\right]&=\left[\!\left[\frac{1}{2}\right]\!\right]+\left(1+\left[\!\left[\frac{3}{2}\right]\!\right]\right)+\left(2+\left[\!\left[\frac{5}{2}\right]\!\right]\right)+\cdots+\left(\frac{n-1}{2}+\left[\!\left[\frac{n}{2}\right]\!\right]\right)\\&=2\left(1+2+\cdots+\frac{n-1}{2}\right)\\&=\frac{n^2-1}{4}=\left[\!\left[\frac{n^2}{4}\right]\!\right]\end{aligned}$$

إذاً $\left[\!\left[n^2/4 \right]\!\right]=\sum_{k=1}^{n}\left[\!\left[k/2 \right]\!\right]$ لجميع الأعداد الطبيعية n.

172. لِنرمز لعدد عناصر المجموعة A بالرمز $|A|$. لاحظ أنه إذا كان $(i,n)=d$، فإنه يمكننا أن نكتب $i=jd$ و $n=md$، حيث j و m عددان صحيحان يحققان $(j,m)=1$. بهذه الملحوظة يصبح لدينا الآتي:

$$\begin{aligned}\left|\{i:1\le i\le n,\ (i,n)=d\}\right| &=\left|\{jd:1\le jd\le md,\ (jd,md)=d\}\right|\\ &=\left|\{jd:1\le j\le m,\ (j,m)=1\}\right|\\ &=\phi(m)\\ &=\phi\left(\frac{n}{d}\right)\end{aligned}$$

173. نُرتِب الأعداد $1\cdot 2,2\cdot 3,3\cdot 4,\cdots,p^k\cdot(p^k+1)$ على الشكل الآتي:

$$\begin{array}{l}1\cdot 2,2\cdot 3,\cdots,(p-1)\cdot p,p\cdot(p+1)\\ (p+1)\cdot(p+2),\cdots,(2p-1)\cdot 2p,2p\cdot(2p+1)\\ \vdots\\ ((i-1)p+1)\cdot((i-1)p+2),\cdots,(ip-1)\cdot ip,ip\cdot(ip+1)\\ \vdots\\ ((p^{k-1}-1)p+1)\cdot(p^{k-1}-1)p+2),\cdots,(p^k-1)\cdot p^k,p^k\cdot(p^p+1)\end{array}$$

نلاحظ أن جميع الأعداد لا تقبل القسمة على p ماعدا آخر عددين في كل صف. وحيث إنَّ عدد الصفوف يساوي p^{k-1} صفاً، فإن عدد الأعداد الأولية نسبياً مع p في المجموعة أعلاه يساوي p^k-2p^{k-1}، أو $p^{k-1}(p-2)$.

174. الأعـداد $n=19^k$، حيـث $k\geq 1$، تحقـق المطلـوب لأن $\phi(n)=19^{k-1}(19-1)=19^{k-1}\times 2\times 9$.

175. إذا كان n يقبل القسمة على عددين أوليين فرديين مُختلفين فإن $4|\phi(n)$ ومـن ثـم $\phi(n)\neq 6$. وإذا كـان $n=2^\alpha$، $\alpha\geq 1$، فـإن $\phi(n)=2^{\alpha-1}\neq 6$. أيضاً إذا كان $n=2^\alpha\cdot p^\beta$، حيث p عدد أولي فـردي و $\alpha\geq 2$ و $\beta\geq 1$ فإن $4|\phi(n)$ ومن ثم $\phi(n)\neq 6$. نستنتج من ذلك أن n يمكن أن تأخذ إحدى الصيغتين الآتيتين

$$n=p^\beta,\quad n=2p^\beta,\quad \beta\geq 1$$

وفي كلتا الحالتين المعادلة $\phi(n)=6$ تُكافئ المعادلة التالية

$$p^{\beta-1}(p-1)=2\cdot 3$$

إذا كـان $p>7$ فـإن $p-1>6$ ومـن ثـم $p^{\beta-1}(p-1)\neq 6$. إذاً فـالقيم المُحتملـة للعـدد الأولي الفـردي p هـي 3 أو 5 أو 7. نجـد بسـهولة أن الحلول هي $(p,\beta)=(3,2),\ (7,1)$ و هذه تُعطينا الحلول الأربعة

$$n=3^2,\ 2\cdot 3^2,\ 7,\ 2\cdot 7$$
$$=9,\ 18,\ 7,\ 14$$

للمعادلة $\phi(n)=6$.

176. إذا كان n يقبل القسمة على عددين أوليين فرديين مُختلفين فإن $4|\phi(n)$ ومـن ثـم $\phi(n)\neq 2\times 7^m$. وإذا كـان $n=2^\alpha$، $\alpha\geq 1$، فـإن $\phi(n)=2^{\alpha-1}\neq 2\times 7^m$. أيضاً إذا كان $n=2^\alpha\cdot p^\beta$، حيـث p عـدد أولي فردي و $\alpha\geq 2$ و $\beta\geq 1$ فإن $4|\phi(n)$ ومن ثم $\phi(n)\neq 2\times 7^m$. نستنتج من ذلك أن n يمكن أن تأخذ إحدى الصيغتين الآتيتين

$$n = p^{\beta}, \quad n = 2p^{\beta}, \quad \beta \geq 1$$

وفي كلتا الحالتين المعادلة $\phi(n) = 2\times 7^m$ تُكافئ المعادلة الآتية

$$p^{\beta-1}(p-1) = 2\times 7^m$$

نُثبت الآن أنه لا يوجد أي حل للمعادلة السابقة.

إذا كان $\beta=1$ فسوف نحصل على $p = 1+2\times 7^m$ وهذا مُستحيل لأن $1+2\times 7^m$ ليس عدداً أولياً $(1+2\times 7^m \equiv 1+2\times 1^m \equiv 3 \equiv 0 \text{ mod } 3)$.

إذا كان $\beta\geq 2$ فإن المعادلة $p^{\beta-1}(p-1) = 2\times 7^m$ تقتضي أن $p \mid 2\times 7^m$ ومن ثم $p=7$ لأن p عدد أولي فردي. هذا يُعطينا $7^{\beta-1}\times 6 = 2\times 7^m$ ومن ثم $3 \mid 7^m$ وهذا مُستحيل.

نستنتج من ذلك كُله أنه لا يوجد أي حل للمعادلة $\phi(n) = 2\times 7^m$ لأي عدد صحيح $m \geq 1$.

177. المعادلة $\phi(n) = \frac{2}{7}n$ تقتضي أن $7\phi(n) = 2n$ ومن ثم $7 \mid 2n$. بما أن $(7,2)=1$ فإن $7 \mid n$. لذا يمكن أن نكتب

$$n = 7^{\gamma}\prod_{i=1}^{r} p_i^{\alpha_i}, \ \gamma \geq 1, \ \alpha_i \geq 1, \ p_i \neq 7, \ 1 \leq i \leq r$$

بالتعويض في المعادلة $\phi(n) = \frac{2}{7}n$ نحصل على المعادلة

$$7^{\gamma-1}(7-1)\prod_{i=1}^{r} p_i^{\alpha_i-1}(p_i-1) = 7^{\gamma-1}\times 2\prod_{i=1}^{r} p_i^{\alpha_i}$$

أو بالتبسيط

$$3\prod_{i=1}^{r}(p_i-1) = \prod_{i=1}^{r} p_i$$

هذا يقتضي أن $3 \mid \prod_{i=1}^{r} p_i$ ومن ثم $p_i = 3$ لعددٍ ما i، حيث $1 \le i \le r$. للتبسيط يمكن أن نأخذ $p_1 = 3$. بالتعويض في المعادلة السابقة عن القيمة $p_1 = 3$ نحصل على المعادلة

$$2\prod_{i=2}^{r}(p_i - 1) = \prod_{i=2}^{r} p_i$$

هذا بدوره يقتضي أن $2 \mid \prod_{i=2}^{r} p_i$ ومن ثم $p_i = 2$ لعددٍ ما i، حيث $2 \le i \le r$. للتبسيط يمكن أن نأخذ $p_2 = 2$. بالتعويض في المعادلة السابقة نحصل على المعادلة

$$\prod_{i=3}^{r}(p_i - 1) = \prod_{i=3}^{r} p_i$$

نلاحظ الآن من المعادلة السابقة أنه إذا كان n يقبل القسمة على عدد أولي مُختلِف عن الأعداد الأولية $2, 3, 7$ فإننا سوف نحصل على المساواة المستحيلة $\prod_{i=3}^{r}(p_i - 1) = \prod_{i=3}^{r} p_i$ (فردي = زوجي.) نستنتج من ذلك أن n لا يمكن أن يقبل القسمة على أعداد أولية مُختلِفة عن الأعداد $2, 3, 7$. أي أن n يجب أن تأخذ الصيغة $n = 2^{\alpha} \times 3^{\beta} \times 7^{\gamma}$. أيضاً نجد بسهولة أنه إذا كان $n = 2^{\alpha} \times 3^{\beta} \times 7^{\gamma}$ فإن $\phi(n) = \frac{2}{7}n$.

178. لنفرض وجود عدد منتهٍ من الأعداد الأولية. ليكن P هو حاصل ضرب هذه الأعداد الأولية. نجد أولاً أنَّ $\phi(P) = 1$ لأن أي عدد أقل من P إما أن يكون عدداً أولياً أو حاصل ضرب أعداد أولية. باستخدام القانون المعطى، نحصل على الآتي:

$$1 = \phi(P) = P\prod_{p \mid P}\left(1 - \frac{1}{p}\right) = \prod_{p \mid P}(p - 1)$$

هذا التناقض الواضح يثبت وجود عدد لا منتهٍ من الأعداد الأولية.

179. لنفرض أنه يوجد عدد أولي p و عدد صحيح $t \geq 2$ بحيث $p^t \mid n$ (وبالضرورة $p^2 \mid n$) و $p^{t+1} \nmid n$. إذاً $p^{t-1}(p-1) = \phi(p^t) \mid \phi(n)$، أي أن $p \mid \phi(n)$. لكن $p \nmid n-1$ (لأن $p \mid n$ و $(n, n-1) = 1$). هذا يقتضي أن $\phi(n) \nmid n-1$. هذا التناقض يكمل الإثبات.

180. لاحظ أولاً أنه إذا كان $p \mid n$ فإن $p \leq n$ ومن ثم $\left(1-\frac{1}{n}\right) \leq \left(1-\frac{1}{p}\right)$. هذا يقتضي الآتي:

$$\frac{\phi(n)}{n} = \prod_{p \mid n}\left(1-\frac{1}{p}\right) \leq \prod_{p \mid n}\left(1-\frac{1}{n}\right) = \left(1-\frac{1}{n}\right)^{\omega(n)}$$

181. لاحظ أولاً أن

- $\phi(n^2) = n^2 \prod_{p \mid n}\left(1-\frac{1}{p}\right) = n\phi(n)$ لجميع القيم $n \geq 2$
- $\phi(n) \leq n-1$ لجميع القيم $n > 1$

هذا يقتضي أن

$$\begin{aligned}\phi(n^2) + \phi((n+1)^2) &= n\phi(n) + (n+1)\phi(n+1) \\ &\leq n(n-1) + (n+1)n \\ &= 2n^2\end{aligned}$$

182. بسبب وجود عدد لانهائي من الأعداد الأولية ذات الصيغة العامة $4k+1$، إذاً فالقيم $n = p = 4k+1$ تحقق الشرط المطلوب:

$$\begin{aligned}\phi(n+1) &= \phi(4k+2) = \phi(2)\phi(2k+1) \\ &= \phi(2k+1) \leq 2k < 4k = \phi(n)\end{aligned}$$

183. حيث إنَّ $\sigma(x) > x$، فإن أي حل x للمعادلة $\sigma(x) = n$ يجب أن يحقق $x < n$، ومن ثم فعدد الحلول للمعادلة المعطاة هو عدد محدود.

184. نكتب أولاً المعادلة على الصيغة: $\sigma(n) - n - 1 = 4$

إذا كانت n تقبل القسمة على عددين أوليين مختلفين p و q فإن

$$4 = \sigma(n) - n - 1 \geq p + q$$

وهذا مستحيل لأن $p + q \geq 2 + 3 = 5$. من ذلك نستنتج أن n لابد أن تكون على الصيغة $n = p^{\alpha}$ حيث p عدد أولي و $\alpha \geq 1$. بسهولة نجد أنه في حالتي $\alpha = 1$ و $\alpha = 2$ فإن $n = p^{\alpha}$ لا تحقق المعادلة المعطاة. إذا كانت $\alpha \geq 3$ فإن

$$4 = \sigma(n) - n - 1 \geq p + p^2$$

وهذا مستحيل لأن $p + p^2 \geq 2 + 2^2 = 6$. إذاً لا يوجد للمعادلة المعطاة أي حل.

185. بملاحظة أن $d \mid n$ إذا و فقط إذا $(n/d) \mid n$، نستنتج ما يلي:

$$\sigma(n) = \sum_{d \mid n} d = \sum_{d \mid n} \frac{n}{d} = n \sum_{d \mid n} \frac{1}{d} \leq n \sum_{k=1}^{n} \frac{1}{k}$$

بالقسمة على n نحصل على المطلوب.

186. عند كتابة $n = \prod_{i=1}^{t} p_i^{k_i}$، وباستخدام قانون $\sigma(n)$ نحصل على الآتي:

$$\sigma(n)=\prod_{i=1}^{t}\frac{p_i^{k_i+1}-1}{p_i-1}=\prod_{i=1}^{t}(1+p_i+\cdots+p_i^{k_i})$$
$$=\prod_{i=1}^{t}p_i^{k_i}(\frac{1}{p_i^{k_i}}+\frac{1}{p_i^{k_i-1}}+\cdots+1)$$
$$=n\prod_{i=1}^{t}\left(\frac{1}{p_i^{k_i}}+\frac{1}{p_i^{k_i-1}}+\cdots+1\right)\ge n\prod_{i=1}^{t}\left(1+\frac{1}{p_i}\right)$$

بالقسمة على n يكمل الإثبات.

187. إذا كان n عدداً مؤلفاً فإنه يوجد عدد d يقسم n بحيث أن $1<d<n$. هذا يقتضي أن $\frac{n}{d}$ أيضاً يقسم n و $1<\frac{n}{d}<n$. بملاحظة أنه إما d أو $\frac{n}{d}$ أكبر من أو يساوي $\sqrt{n}$ (إذا كان $d\le\sqrt{n}$ فإن $\frac{n}{d}\ge\frac{n}{\sqrt{n}}=\sqrt{n}$) فإننا نستنتج أن $\sigma(n)>n+d+\frac{n}{d}>n+\sqrt{n}$.

188. لِنضع $m=3n+2$. لأي قاسم موجب d للعدد m يوجد قاسم موجب e للعدد m بحيث يكون $m=de$. إذا كان $d\equiv 1 \bmod 3$ فإن $e\equiv 2 \bmod 3$ (لأن $m\equiv 2 \bmod 3$.) وإذا كان $d\equiv 2 \bmod 3$ فإن $e\equiv 1 \bmod 3$ (لأن $m\equiv 2 \bmod 3$.) في كلتا الحالتين $d+e\equiv 0 \bmod 3$. بملاحظة أنَّ

$$2\sigma(m)=\sum_{d\mid m}d+\sum_{e\mid m}e=\sum_{(d,e),de=m}(d+e)\equiv 0 \bmod 3$$

حيث أن المجموع الأخير يجري على جميع الأزواج المرتبة (d,e) التي تُحقِق $d>0$ و $e>0$ و $de=m$، نستنتج من ذلك أن $3\mid 2\sigma(m)$. بما أن $(3,2)=1$ فإن $3\mid\sigma(m)$، أي أن $3\mid\sigma(3n+2)$.

189. لتكن $n_1, n_2, \cdots, n_{\tau(n)}$ القواسم الموجبة للعدد n. إذاً الأعداد $kn_1, kn_2, \cdots, kn_{\tau(n)}$ هي قواسم للعدد kn وجميعها أكبر من 1. من ذلك نستنتج أن

$$\sigma(kn) \ge kn_1 + kn_2 + \cdots + kn_{\tau(n)} + 1 = k\,\sigma(n) + 1$$

بالقسمة على kn نحصل على المطلوب:

$$\frac{\sigma(kn)}{kn} \ge \frac{\sigma(n)}{n} + \frac{1}{kn} > \frac{\sigma(n)}{n}$$

190. بما أن $\tau(n) = 30 = 2\times3\times5 = 2\times15 = 3\times10 = 5\times6$، فإنه يمكننا أن نستنتج من القانون العام للدالة $\tau(n)$ أن الصيَغ الممكنة للعدد n هي

$$n = p^{29},\, pq^2r^4,\, pq^{14},\, p^2q^9,\, p^4q^5$$

حيث إنَّ p, q, r أعداد أولية. للحصول على أصغر قيمة للعدد n، فإن القيم المحتملة للأعداد الأولية p, q, r لابد أن تكون 2,3,5 (أصغر الأعداد الأولية). بتعويض القيم الممكنة للأعداد الأولية p, q, r في الأعداد n أعلاه، نجد أن أصغر الحلول هو $n = pq^2r^4 = 5\times3^2\times2^4 = 720$.

191. بما أن $\tau(n) = 4 = 2\times2$ فإنه إما $n = p^3$ أو $n = pq$ حيث p و q عددان أوليان. إذا كان $n = p^3$ فإن $\sigma(n) = 72$ يقتضي أن

$$1 + p + p^2 + p^3 = 72 \Rightarrow p^3 < 72 \Rightarrow p = 2,\ 3$$

أي أن $n = 8,\ 27$ و كلا العددين لا يُحقِّق المعادلة $\sigma(n) = 72$. الآن لِنفرض أن $n = pq$ و $p < q$. المعادلة $\sigma(n) = 72$ تقتضي أن

$$(1+p)(1+q)=72$$

بما أن $72=1\times72=2\times36=3\times24=4\times18=8\times9$ فإننا نحصل على احتمالين يؤديان إلى حلين هما

$$\begin{cases}1+p=3,\ 1+q=24\\1+p=4,\ 1+q=18\end{cases}$$

أي أن $p=2$ و $q=23$ ومن ثم $n=pq=46$ و $p=3$ و $q=17$ ومن ثم $n=pq=51$. إذاً يوجد عددان طبيعيان يُحقِّقان المعادلتين $\tau(n)=4$ و $\sigma(n)=72$ معاً هما $n=46$ و $n=51$.

192. حيث إنَّ $4k+1$ و $6k+1$ عددين أوليين فإن $\tau(4k+1)=2$ و $\tau(6k+1)=2$. بإجراء الحسابات الآتية

$$\tau(12k+2)=\tau(2(6k+1))=\tau(2)\tau(6k+1)=2\times2=4$$
$$\tau(12k+3)=\tau(3(4k+1))=\tau(3)\tau(4k+1)=2\times2=4$$

نستنتج أن $\tau(12k+2)=\tau(12k+3)$.

193. إذا كان $n=ab$ فإنه إما $a\le\sqrt{n}$ أو $b\le\sqrt{n}$. هذا يعني أنه لأي عدد n يوجد قاسم أقل من أو يساوي $\sqrt{n}$. هذا يقتضي أن العدد الممكن لقواسم n والتي هي أقل من أو يساوي $\sqrt{n}$ هو أقل من أو يساوي $\sqrt{n}$. بالملحوظة المعطاة أعلاه، يقابل أي قاسم أقل من أو يساوي $\sqrt{n}$ قاسم آخر أكبر من أو يساوي $\sqrt{n}$. نستنتج من ذلك أن $\tau(n)\le2\sqrt{n}$.

194. لنأخذ عدداً أولياً p. إذا كان n عدداً زوجياً فإنه يمكننا أن نكتب

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

وإذا كان $n>1$ عدداً فرديا فإنه يمكننا أن نكتب

$$n=\frac{n+1}{2}+\frac{n-1}{2}=\tau(p^{\frac{n-1}{2}})+\tau(p^{\frac{n-3}{2}})$$

195. إذا كان $n=\underbrace{1111\cdots11}_{2010}$ فإن $3|n$ و $3^2\nmid n$. هذا يقتضي أن $\tau(3)|\tau(n)$. حيث إنَّ $\tau(3)=2$، إذاً $\tau(n)$ عدد زوجي.

196. من ضمن أي أربعة أعداد صحيحة موجبة $n,n+1,n+2,n+3$ لابد أن يكون أحدها قابلاً للقسمة على 4. فلو فرضنا على سبيل المثال أن $4|n$ فإنه إما أن يكون $n=4$ أو $n=4k$، حيث $k>1$ عدد صحيح. إذا كان $n=4$ فإن $\tau(n)=3$، وإذا كان $n=4k$ فإن الأعداد $1,2,4,k\ ,2k\ ,4k$ هي قواسم للعدد n ومن ثم فإن $\tau(n)>4$. إذاً في كلتا الحالتين $\tau(n)\neq 4$ ومن ثم فإننا نستنتج أنه لا يوجد عدد صحيح $n\geq 1$ يُحقِّق المعادلة $\tau(n)=\tau(n+1)=\tau(n+2)=\tau(n+3)=4$.

197. لنكتب $n=p^{\alpha_1}\cdot p_2^{\alpha_2}\cdots p_r^{\alpha_r}$، حيث p هو أصغر عدد أولي يقسم n. هذا يعطي $\omega(n)=r$. لأن

$$n\geq p^{\alpha_1}\cdot p^{\alpha_2}\cdots p^{\alpha_r}\geq p^r=p^{\omega(n)}$$

إذاً بأخذ اللوغاريثم للطرفين نحصل على المطلوب.

198. بملاحظة أولاً أنه يوجد عدد لانهائي من الأعداد الأولية ذات الصيغة العامة $6k+1$، إذاً فالقيم $n=6k$ تحقق الشرط المطلوب: $\omega(n)=\omega(6k)\geq\omega(6)=2$ و $\omega(n+1)=\omega(6k+1)=1$.

199. لِنفرض أن $\omega(2^n-1)\geq n$. هذا يقتضي أن 2^n-1 يقبل القسمة على الأقل على عدد n من الأعداد الأولية الفردية، ولتكن $p_1,p_2,\cdots,p_n$. نستنتج من ذلك أن

$$2^n-1\geq p_1\times p_2\times\cdots\times p_n>2\times2\times\cdots\times2=2^n$$

وهذا مُستحيل. إذاً $\omega(2^n-1)<n$.

200. الإثبات يتم بملاحظة أنه لأي عدد n، أحد الأعداد n, $n+2$, $n+5$, $n+7$ يقبل القسمة على 4. وإثبات ذلك يتم بدراسة الصيغ الممكنة للعدد n وهي $4k$, $4k+1$, $4k+2$, $4k+3$.

201. لاحظ أولاً أنه بما أن n عدد فردي، فإن $a+b$ يقسم $c^m=a^n+b^n$. هذا يقتضي أن أي عدد أولي يقسم $a+b$ سوف يقسم أيضاً c^m ومن ثم يقسم c. الآن لنفرض أنَّ $\mu(a+b)\neq 0$. هذا يعني أن جميع الأعداد الأولية التي تقسم $a+b$ مرفوعة للأُس 1. باستخدام الملحوظة السابقة، نستنتج أن $a+b$ يقسم c وهذا بدوره يقتضي أن $a+b\leq c$. لكن هذا مستحيل لأن $c<a+b$ (لأن $c^n<c^m=a^n+b^n<(a+b)^n$).
هذا التناقض يقتضي أن $\mu(a+b)=0$.

202. لنضع $F(n)=\sum_{d|n}\mu(d)\omega(d)$. حيث إنَّ $\mu(n)$ و $\omega(n)$ دالتان ضربيتان فإن $\mu(n)\omega(n)$ دالة ضربية ومن ثم $F(n)$ دالة ضربية أيضاً (نظرية 35). لِذا نحسب أولاً $F(p^k)$ حيث p عدد أولي و $k\geq 1$ عدد صحيح:

$$F(p^k)=\sum_{d|p^k}\mu(d)\omega(d)=\sum_{i=0}^{k}\mu(p^i)\omega(p^i)=1-1=0$$

الآن إذا كان $n=\prod_{i=1}^{r} p_i^{k_i}$ فإن

$$F(n)=\prod_{i=1}^{r} F(p_i^{k_i})=\prod_{i=1}^{r} 0=0$$

أي أن $\sum_{d|n}\mu(d)\omega(d)=0$.

203. لِنضع $F(n)=\sum_{d|n}\frac{\mu^2(d)}{\phi(d)}$. حيث إنَّ μ و ϕ دالتان ضربيتان فإن $\frac{\mu^2}{\phi}$ دالة ضربية ومن ثم F أيضاً دالة ضربية (نظرية 35). لِذا نحسب أولاً $F(p^k)$ حيث p عدد أولي و $k\geq 1$ عدد صحيح:

$$F(p^k)=\sum_{d|p^k}\frac{\mu^2(d)}{\phi(d)}=\sum_{i=0}^{k}\frac{\mu^2(p^i)}{\phi(p^i)}=1+\frac{1}{p-1}=\frac{p}{p-1}$$

الآن إذا كان $n=\prod_{i=1}^{r} p_i^{\alpha_i}$ فإن

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

$$=\prod_{p|n}\left(1-\frac{1}{p}\right)^{-1}=\frac{n}{\phi(n)}$$

أي أن $\frac{n}{\phi(n)}=\sum_{d|n}\frac{\mu^2(d)}{\phi(d)}$ وبهذا يتم الإثبات.

204. إذا كان $n=p^{\alpha}$ حيث p عدد أولي و $\alpha\geq 1$ عدد صحيح، فإن

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

حيث إنَّ ϕ و σ دالتان ضربيتان فإنه بكتابة $n=\prod_{i=1}^{r} p_i^{\alpha_i}$، نحصل على

المطلوب:

$$\phi(n)\sigma(n)=\prod_{i=1}^{r}\phi(p_i^{\alpha_i})\sigma(p_i^{\alpha_i})<\prod_{i=1}^{r}p_i^{2\alpha_i}=n^2$$

205. مجموعة قواسم جميع الأعداد $1,2,3,\cdots,n$ هي $\{1,2,3,\cdots,n\}$. نقوم الآن بحساب عدد المرات التي تم حساب كل قاسم في المجموع

$$\tau(1)+\tau(2)+\tau(3)+\cdots+\tau(n)$$

القاسم 1 يقسم جميع الأعداد، ومن ثم فإن عدد المرات التي تم حساب القاسم 1 في المجموع أعلاه يساوي $n=\left[\!\left[\frac{n}{1}\right]\!\right]$.

القاسم 2 يقسم جميع الأعداد الزوجية الموجودة من ضمن الأعداد $1,2,3,\cdots,n$، ومن ثم فإن عدد المرات التي تم حساب القاسم 2 في المجموع أعلاه يساوي $\left[\!\left[\frac{n}{2}\right]\!\right]$.

القاسم 3 يقسم جميع مضاعفات العدد 3 الموجودة من ضمن الأعداد $1,2,3,\cdots,n$، ومن ثم فإن عدد المرات التي تم حساب القاسم 3 في المجموع أعلاه يساوي $\left[\!\left[\frac{n}{3}\right]\!\right]$. وهكذا حتى نصل إلى القاسم n، حيث إنَّ عدد المرات التي تم حسابه في المجموع أعلاه يساوي $1=\left[\!\left[\frac{n}{n}\right]\!\right]$. إذاً نحصل على

$$\tau(1)+\tau(2)+\tau(3)+\cdots+\tau(n)=\left[\!\left[\frac{n}{1}\right]\!\right]+\left[\!\left[\frac{n}{2}\right]\!\right]+\left[\!\left[\frac{n}{3}\right]\!\right]+\cdots+\left[\!\left[\frac{n}{n}\right]\!\right]$$

206. نبدأ الحل بالملحوظة التالية: إذا كان $(m,n)=1$ و $d^2\mid mn$

فإنه يوجد عددان صحيحان موجبان وحيدان d_1 و d_2 بحيث يكون $d_1^2 \mid m$ و $d_2^2 \mid n$ و $d = d_1 d_2$ و $(d_1, d_2) = 1$. نترك إثبات ذلك للقارئ. الآن نأخذ عددين صحيحين موجبين m و n يُحقِّقان $(m,n) = 1$ و نريد أن نُثبت أن

$$G(mn) = G(m)G(n)$$

باستخدام الملحوظة أعلاه نقوم بإجراء الآتي:

$$\begin{aligned}
G(mn) &= \sum_{d^2 \mid mn} f(d) \\
&= \sum_{\substack{d_1^2 \mid m \\ d_2^2 \mid n}} f(d_1 d_2) = \sum_{\substack{d_1^2 \mid m \\ d_2^2 \mid n}} f(d_1) f(d_2) \\
&= \sum_{d_2^2 \mid n} \left(\left[\sum_{d_1^2 \mid m} f(d_1) \right] f(d_2) \right) \\
&= \left[\sum_{d_1^2 \mid m} f(d_1) \right] \sum_{d_2^2 \mid n} f(d_2) = G(m)G(n)
\end{aligned}$$

هذا يُثبت أن G دالة ضربية.

207. إذا كان n عدداً تاماً فإن $\sigma(n) = 2n$. باستخدام السؤال رقم 189 نحصل على العلاقة $\sigma(kn) > k\,\sigma(n)$. لذا نستنتج أن

$$\sigma(kn) > k\,\sigma(n) = k(2n) = 2kn$$

ومن ثم فإن العدد nk عددٌ زائد.

208. نُريد أن نُثبت أن $\sigma(2^k \times 11) > 2 \times (2^k \times 11)$. لاحظ أن

$$\begin{aligned}
\sigma(2^k \times 11) &= \sigma(2^k)\sigma(11) = (2^{k+1} - 1) \times (1 + 11) \\
&= 2^{k+1} \times 11 + 2^{k+1} - 12 > 2^{k+1} \times 11
\end{aligned}$$

حيث إنَّ المتباينة صحيحة لأن $2^{k+1}-12>0$ وذلك لأن $k\geq 3$. من ذلك نستنتج أن العدد 11×2^{k} عددٌ زائد لجميع الأعداد الصحيحة $k\geq 3$.

209. مُعطى السؤال يقتضي أن $n=2^{p-1}(2^{p}-1)$ حيث p و $2^{p}-1$ عددان أوليان فرديان. بما أن p عدد فردي، فإن $3|2^{p-1}-1$ ومن ثم $2^{p-1}=3k+1$، حيث k عدد صحيح موجب. بالضرب في 2 نحصل على $2^{p}=6k+2$. بالحساب قياس 9 نحصل على المطلوب:

$$n=2^{p-1}(2^{p}-1)=(3k+1)(6k+1)=18k^{2}+9k+1\equiv 1 \bmod 9$$

210. بحساب قيمة $\sigma(p^{k}q^{l})$ نحصل على الآتي:

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

بما أن $2<p<q$ فإن $p\geq 3$ و $q\geq 5$. هذا بدوره يعطينا التالي:

$$1-p^{-(k+1)}<1,\ 1-q^{-(l+1)}<1$$
$$p\geq 3\Rightarrow p^{-1}\leq 3^{-1}\Rightarrow 1-p^{-1}\geq 1-3^{-1}\Rightarrow\frac{1}{1-p^{-1}}\leq\frac{3}{2}$$
$$q\geq 5\Rightarrow q^{-1}\leq 5^{-1}\Rightarrow 1-q^{-1}\geq 1-5^{-1}\Rightarrow\frac{1}{1-q^{-1}}\leq\frac{5}{4}$$

نستنتج من ذلك أن

$$\sigma(p^{k}q^{l})\leq\frac{15}{8}p^{k}q^{l}<2p^{k}q^{l}$$

ومن ثم فإن العدد $p^{k}q^{l}$ عدد ناقص.

211. من السؤال السابق نستنتج أنه لكي يكون $n = p^2q$ عدداً تاماً فلابد أن يكون $p = 2$ أو $q = 2$، أي أن n عدد تام زوجي. هـذا يقتضي أن

$$p^2q = 2^{r-1}(2^r - 1)$$

حيث إنَّ r و $2^r - 1$ عددان أوليان. إذا كان $p = 2$ فإن $2^2q = 2^{r-1}(2^r - 1)$ يقتضي أن $r = 3$ و $q = 7$، أي أن $n = 2^2 \times 7 = 28$. وإذا كان $q = 2$ فإن $p^2 \times 2 = 2^{r-1}(2^r - 1)$ يقتضي أن $r = 2$ ومن ثم $p^2 = 5$ وهذا مستحيل.

إذاً العدد 28 هو العدد التام الوحيد الذي يمكن كتابته على الصيغة العامة p^2q حيث $p \neq q$ عددان أوليان.

212. نُريد أن نُثبت أن $\sigma(2p(2p+1)) < 2 \times 2p(2p+1)$ إذا كان $p > 3$ و $2p + 1$ عددين أوليين. حيث إنَّ

$$\begin{aligned}\sigma(2p(2p+1)) &= \sigma(2)\sigma(p)\sigma(2p+1)\\ &= 3(p+1)(2p+2) = 6(p+1)^2\end{aligned}$$

فإن الإثبات سوف يتم إذا أثبتنا أن $6(p+1)^2 < 2 \times 2p(2p+1)$. لكن هذه المتباينة مُكافئة للمتباينة $3 < p^2 - 4p$ وهي متباينة صحيحة لأن $p \geq 5$: $p^2 - 4p = p(p-4) > 3 \times 1 = 3$. من ذلك نستنتج أن العدد $2p(2p+1)$ عدد ناقص.

213. إذا كان $q = 2$، فإن العدد $q(q+1) = 6$ عددٌ تام. لنفرض الآن أن $q > 2$ عددٌ أولي. إذا كان $q(q+1)$ عدداً تاماً، فبما أنه عدد زوجي فإنه يوجد عدد أولي p بحيث أن $2^p - 1$ عدد أولي و

$$q(q+1)=2^{p-1}(2^p-1)$$

هذا يقتضي أن $q=2^p-1$ و $q+1=2^{p-1}$ ومن ثم $2^{p-1}=2^p$ أو $1=2$ وهذا مستحيل. إذاً يوجد عدد أولي وحيد هو $q=2$ يجعل العدد $q(q+1)$ عدداً تاماً.

214. لنفرض أن العدد $n=pqr$ عدد تام، أي أن $\sigma(n)=2n$، أو

$$(p+1)(q+1)(r+1)=2pqr$$

إذا كانت الأعداد p و q و r جميعها فردية فإن المعادلة أعلاه غير ممكنة التحقق لأنه في هذه الحالة $2\|2pqr$ بينما $8|(p+1)(q+1)(r+1)$. إذاً لابد أن يكون أحد الأعداد p أو q أو r عدداً زوجياً. لنفرض أن $p=2$. في هذه الحالة المعادلة أعلاه تصبح

$$3(q+1)(r+1)=4qr$$

هذا يقتضي أن $3|qr$ ومن ثم $q=3$ أو $r=3$ لأن q و r عددان أوليان. في كلتا الحالتين، عند التعويض في المعادلة السابقة ومن ثم التبسيط نحصل على $0=1$ وهذا مستحيل. هذا يُثبت أن العدد $n=pqr$ ليس عدداً تاماً.

215. من مُعطى السؤال يمكن أن نكتب

$$P=2^{p-1}(2^p-1)$$
$$Q=2^{q-1}(2^q-1)$$

حيث p و q عددان أوليان. الشرط $6<P<Q$ يقتضي أن $2<p<q$، أي أن p و q عددان أوليان فرديان ومن ثم $q-p\ge 2$. هذا يقتضي أن

$2^{q-p} \geq 4$ أو $2^q \geq 4\times 2^p$.

نستنتج من ذلك أن $2^q - 1 \geq 4\times 2^p - 1$. لكن حيث إنَّ $4\times 2^p - 1 > 4(2^p - 1)$ إذاً نحصل على $2^q - 1 > 4(2^p - 1)$ أو

$$\frac{2^q - 1}{2^p - 1} > 4$$

الآن

$$\frac{Q}{P} = 2^{q-p} \times \frac{2^q - 1}{2^p - 1} > 4\times 4$$

ومنه نحصل على $Q > 16P$ وهو المطلوب.

216. إذا كان (x, y, z) ثلاثي فيثاغورس بدائي فإن

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

حيث r و s عددان صحيحان موجبان أحدهما فردي و الآخر زوجي، و $r > s$ و $(r, s) = 1$. هذا يقتضي أن $r^2 - s^2$ و $r^2 + s^2$ عددان فرديان ومن ثم $x \neq 8$ و $z \neq 8$. يبقى احتمال واحد هو $y = 2rs = 8$، أي أن $rs = 4$. بسبب الشروط التي يحققها r و s نستنتج أنه لابد أن يكون $r = 4$ و $s = 1$. هذا يُعطينا الثلاثي $(x, y, z) = (15,8,17)$ وهو الثلاثي الوحيد الذي يُحقِّق شرط السؤال.

217. أضلاع مثلث قائم الزاوية المطلوب معطاة كثلاثية فيثاغورس (x, y, z). مساحة هذا المثلث A تساوي $A = \frac{1}{2}xy$. حيث إنَّ $A = 30$، إذاً يُصبح لدينا المعادلة $xy = 60$. لهذه المعادلة 12 حلاً:

$$(x,y)=(1,60),(2,30),(3,20),(4,15),(5,12),(6,10),$$
$$(60,1),(30,2),(20,3),(15,4),(12,5),(10,6)$$

الحل الوحيد الذي يُعطينا مثلثاً قائم الزاوية هو $(x,y)=(5,12)$ لأن y عدد زوجي. بما أن $5^2+12^2=13^2$، إذاً يوجد مثلث واحد يُحقِّق السؤال وهو المثلث الذي أضلاعه هي $(x,y,z)=(5,12,13)$.

218. أضلاع مثلث قائم الزاوية المطلوب يُكوِّن ثلاثية فيثاغورس (x,y,z):

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

حيث k عدد صحيح موجب، و r و s عددان صحيحان موجبان أحدهما فردي والآخر زوجي، و $r>s$، و $(r,s)=1$. بما أن قيمة المحيط تساوي 30، فإن $x+y+z=30$، أي

$$kr(r+s)=15$$

هذا يقتضي أن $k\mid 15$ ومن ثم $k=1,3,5,15$.

في حالة $k=1$ يصبح لدينا المعادلة $r(r+s)=15$ والتي حلولها هي

$$(r,s)=(1,14),(3,2),(5,-2),(15,-14)$$

لكن بملاحظة الشروط التي تحققها r و s نجد أن حل المعادلة $r(r+s)=15$ هو $(r,s)=(3,2)$ فقط. هذا بدوره يُنتج الحل $(x,y,z)=(5,12,13)$.

بطريقةٍ مُشابهه نجد أنه في الحالات $k=3,5,15$ لا ينتج أي ثلاثي يُحقِّق شرط السؤال. إذاً المثلث المطلوب والذي يُحقِّق شرط السؤال هو

المثلث ذو الثلاثية $(x, y, z) = (5,12,13)$.

219. أضلاع مثلث قائم الزاوية المطلوب يُكون ثلاثية فيثاغورس (x, y, z):

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

حيث k عدد صحيح موجب، و r و s عددان صحيحان موجبان أحدهما فردي والآخر زوجي، و $r > s$، و $(r, s) = 1$. إذا كانت قيمة المساحة تُساوي قيمة المحيط، فإن $\frac{1}{2}xy = x + y + z$، أو

$$ks(r - s) = 2$$

هذا يقتضي أن $k \mid 2$ ومن ثم $k = 1$ أو $k = 2$. إذا كان $k = 1$ فالمعادلة أعلاه تصبح $s(r - s) = 2$ وحلها هو $(r, s) = (3,2)$. هذا يعطي الثلاثية $(x, y, z) = (5,12,13)$. وإذا كان $k = 2$ فالمعادلة أعلاه تصبح $s(r - s) = 1$ وحلها $(r, s) = (2,1)$. هذا يعطي الثلاثية $(x, y, z) = (6,8,10)$. إذاً يوجد مثلثان يُحقّقان شرط السؤال وهما معطيان بالثلاثيتين $(x, y, z) = (5,12,13), (6,8,10)$.

220. لا يوجد أي مثلث قائم الزاوية يُحقّق شرط السؤال لأنه إذا كانت ثلاثية فيثاغورس (x, y, z) تُمثل أضلاع مثل هذا المثلث، فإن $\sin 60^\circ = x / z$ أو $\sin 60^\circ = y / z$ وكلا القيمتين x / z و y / z يُمثلان عددين نسبيين، بينما $\sin 60^\circ = \sqrt{3} / 2$ عدد غير نسبي.

221. بملاحظة أن

$$M_n = 2^n - 1 = (2^{n-1})^2 - (2^{n-1} - 1)^2$$

فإنه بأخذ $r = 2^{n-1}$ و $s = 2^{n-1} - 1$ في نظرية 39 نحصل على مثلث فيثاغورس بدائي (x, y, z) حيث

$$x = M_n$$
$$y = 2^n M_{n-1}$$
$$z = 2^{2n-1} - M_n$$

222. إذا كان (x, y, z) ثلاثي فيثاغورس يُحقق $y = kx$، حيث $k > 0$، فإن المعادلة $x^2 + y^2 = z^2$ سوف تُصبِح $x^2(1+k^2) = z^2$. من النظرية الأساسية للحساب (نظرية 11) نستنتج أنه لابد أن يكون $1+k^2$ مربعاً كاملاً، أي أن يوجد عدد صحيح موجب l يُحقق $1+k^2 = l^2$، أي أن $(l-k)(l+k) = 1$. بما أن $l > 0$ و $k > 0$ فإننا نحصل على $l + k = 1$ و $l - k = 1$ ومن ثم $l = 1$ و $k = 0$ وهذا مستحيل لأن $k > 0$. إذاً لا يوجد أي ثلاثي فيثاغورس يُحقق شرط السؤال.

223. إذا كان (x, y, z) ثلاثي فيثاغورس بدائي فإن

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

حيث r و s عددان صحيحان موجبان أحدهما فردي والآخر زوجي، و $r > s > 0$ و $(r,s) = 1$. نريد x مربعاً كاملاً، أي $x = t^2$ حيث $t > 0$ عدد صحيح. هذا يُنتِج المعادلة $t^2 = r^2 - s^2$، أو

$$t^2 + s^2 = r^2$$

هذا يقتضي أن (لاحظ أنه بما أن x عدد فردي فإن t عدد فردي)

$$t = m^2 - n^2 ,\ s = 2mn ,\ r = m^2 + n^2$$

حيث m و n عددان صحيحان موجبان أحدهما فردي و الآخر زوجي، و $m > n > 0$ و $(m,n) = 1$. نستنتج من ذلك أن الثلاثيات (x,y,z) المطلوبة هي

$$\begin{cases} x = (m^2 - n^2)^2 \\ y = 4mn(m^2 + n^2) \\ z = m^4 + 6m^2n^2 + n^4 \end{cases}$$

224. إذا كان (x,y,z) ثلاثي فيثاغورس بدائي فإن

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

حيث r و s عددان صحيحان موجبان أحدهما فردي والآخر زوجي و $r > s$ و $(r,s) = 1$. إذا كان $z = y + 9$ فإن $r^2 + s^2 = 2rs + 9$. هذا يقتضي أن $(r - s)^2 = 9$ ومنه $r = s \pm 3$. بما أن $r > s > 0$ فإن $r = s + 3$. وبما أن $(r,s) = 1$ فلابد أن يكون $(s,3) = 1$، وذلك بدراسة الحالات المحتملة لقيمة s: $s = 3k\ ,\ 3k + 1,\ 3k + 2$. إذاً ثلاثيات فيثاغورس البداية (x,y,z) التي تُحقّق شرط السؤال معطاة على النحو الآتي:

$$x = 6s + 9$$
$$y = 2s^2 + 6s$$
$$z = 2s^2 + 6s + 9$$

حيث $s>0$ و $(s,3)=1$.

225. نلاحظ من المعادلة $x^2+y^2=4z^2$ مبدئياً أنه إذا كان $x=2k+1$ و $y=2l+1$ عددين فرديين فإن $2\|x^2+y^2$ ومن ثم $x^2+y^2\neq 4z^2$. أيضاً لا يمكن أن يكون أحد المقدارين x أو y فردياً و الآخر زوجياً و إلا سوف نحصل المساواة المستحيلة (زوجي = فردي). إذاً لابد أن يكون x و y عددين زوجيين، و لنكتب $x=2x_1$ و $y=2y_1$. بالتعويض في المعادلة $x^2+y^2=4z^2$ نحصل على المعادلة

$$x_1^2+y_1^2=z^2$$

نستنتج أن (نتيجة 40)

$$x_1=k(r^2-s^2),\ y_1=2krs,\ z=k(r^2+s^2)$$

ومن ثم

$$x=2k(r^2-s^2),\ y=4krs,\ z=k(r^2+s^2)$$

حيث $k>0$ عدد صحيح و r و s عددان صحيحان موجبان أحدهما فردي و الآخر زوجي، و $r>s>0$ و $(r,s)=1$.

226. نلاحظ أولاً أنه إذا كان d يقسم أي عددين من الأعداد x، y، z فإنه بقسم العدد الثالث:(مثلاً، إذا كان $d\mid x$ و $d\mid z$ فإن $d^2\mid x^2$ و $d^2\mid z^2$ ومن ثم $d^2\mid 3y^2$. باستخدام مثال 8، نجد أن $d\mid y$). نستنتج من ذلك أن $(x,y)=(x,z)=(y,z)=(x,y,z)$. بحذف العوامل المشتركة، يمكن أن نفرض أن

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

ثانياً: x عدد فردي و أحد العددين y و z عدد فردي والآخر عدد زوجي: إذا كان x عدداً زوجياً، فلابد أن يكون y و z عددين فرديين (لأن $1=(x,z)=(x,y)$). بحساب المعادلة $x^2+3y^2=z^2$ قياس 4 نحصل على $0+3(1)\equiv 1 \bmod 4$، وهذا مستحيل. إذاً لابد أن يكون x عدداً فردياً ومن ثم أحد العددين y و z عدد فردي والآخر عدد زوجي.

الآن لنكتب المعادلة على الصورة

$$3y^2=(z-x)(z+x)............(*)$$

ولنضع $g=(z-x,z+x)$. إذاً $g\,|\,z-x$ و $g\,|\,z+x$ يقتضي $g\,|\,2z$ و $g\,|\,2x$ ومن ثم $g\,|\,(2x,2z)=2(x,z)=2$، أي أنه إما $g=1$ أو $g=2$.

الحالة الأولى: $g=1$. في هذه الحالة x عدد فردي و z عدد زوجي و y عدد فردي. من المعادلة (*) نحصل على إما

$$z-x=3a^2,\ z+x=b^2$$

أو

$$z-x=b^2,\ z+x=3a^2$$

وهذا يعطينا على التوالي الحلين $(x,y,z)=(\frac{\pm(b^2-3a^2)}{2},ab,\frac{b^2+3a^2}{2})$. بما أن $x>0$ فإنه يمكننا أن ننظر لهذين الحلين كحلٍ واحد هو $(x,y,z)=(\frac{|b^2-3a^2|}{2},ab,\frac{b^2+3a^2}{2})$ حيث a و b عددان فرديان

و $(3a,b)=1$.

الحالة الثانية: $g=2$. في هذه الحالة x عدد فردي و z عدد فردي و y عدد زوجي. نكتب المعادلة (*) على الصورة

$$3\left(\frac{y}{2}\right)^2=\left(\frac{z-x}{2}\right)\left(\frac{z+x}{2}\right)$$

حيث إن $((z-x)/2,(z+x)/2)=1$، فعند اتباع نفس الخطوات أعلاه، نحصل على الحل $(x,y,z)=(|b^2-3a^2|,2ab,b^2+3a^2)$ حيث a و b عددان أحدهما فردي والآخر زوجي و $(3a,b)=1$.

227. نفرض أنه يوجد حلٌّ صحيحٌ موجب (x_0,y_0,z_0) للمعادلة $3x^2+7y^2=z^2$. كما في السؤال السابق يمكن أن نفرض أنه لا يوجد أي عامل مشترك أكبر من الواحد لأي من الأعداد x_0 و y_0 و z_0، أي أن

$$(x_0,y_0)=(x_0,z_0)=(y_0,z_0)=(x_0,y_0,z_0)=1$$

هذا يقتضي أن $(x_0,7)=(z_0,7)=1$. الآن بما أن $3x_0^2+7y_0^2=z_0^2$ فإن $3x_0^2\equiv z_0^2 \bmod 7$. هذا يقتضي أن

$$1=\left(\frac{z_0^2}{7}\right)=\left(\frac{3x_0^2}{7}\right)=\left(\frac{3}{7}\right)\left(\frac{x_0^2}{7}\right)=\left(\frac{3}{7}\right)$$

وهذا مستحيل لأن

$$\left(\frac{3}{7}\right)=(-1)^{\frac{3-1}{2}\frac{7-1}{2}}\left(\frac{7}{3}\right)=-\left(\frac{1}{3}\right)=-1$$

نستنتج من ذلك أنه لا توجد حلول صحيحة موجبة للمعادلة $3x^2+7y^2=z^2$.

228. نلاحظ أولاً أنه إذا كان $y=1$ فإن x ممكن أن تكون أي عدد صحيح موجب، أي أن $(x,y)=(n,1)$، حيث n عدد صحيح موجب، تُمثِّل حلولاً للمعادلة $x^y=xy$.

الآن نفرض أن $y\neq 1$، أي أن $y\geq 2$. ليكن p عدداً أولياً.

إذا كان $p\mid y$ فإن $p\mid x$ (لأن $x^y=xy$).

إذا كان $p\mid x$ فإن $p\mid y$: لِنفرض أن $p^t\| x$ حيث $t\geq 1$ عدد صحيح. هذا يقتضي أن $x=p^t x_1$ حيث $(p,x_1)=1$. بالتعويض في المعادلة $x^y=xy$ نحصل على $p^{yt}x_1^y=p^t x_1 y$ أو $p^{t(y-1)}x_1^{y-1}=y$ من ثم $p\mid y$ لأن $t\geq 1$ و $y-1\geq 1$.

نستنتج من ذلك أن x و y لهما نفس العوامل الأولية:

$$x=\prod_{i=1}^{r}p_i^{\alpha_i}\ ,\ \ y=\prod_{i=1}^{r}p_i^{\beta_i}\ ,\ \alpha_i\geq 1,\ \beta_i\geq 1$$

بالتعويض في المعادلة $x^y=xy$ نحصل على $\alpha_i y=\alpha_i+\beta_i$ أو

$$\alpha_i(y-1)=\beta_i\ ,\quad 1\leq i\leq r$$

الآن إذا كان $y-1\neq 1$ (أي أن $y\geq 3$) فإن $y-1\leq \beta_i$ ومن ثم نحصل على

$$y=\prod_{i=1}^{r}p_i^{\beta_i}\geq \prod_{i=1}^{r}2^{y-1}=2^{r(y-1)}\geq 2^{y-1}>y$$

وهذا تناقض واضح.(لاحظ أنه بما أن $y-1\neq 1$ فإن $2^{y-1}=(1+1)^{y-1}=1+(y-1)+\cdots+1>y$). إذاً لابد أن يكون $y-1=1$ ومن ثم $y=2$. هذا يُعطينا المعادلة $x^2=2x$ ومن ثم $x=2$ (لأن $x>0$).

نستنتج من ذلك أن الحلول الصحيحة الموجبة للمعادلة $x^y = xy$ هي $(x,y) = (n,1),(2,2)$ حيث n عدد صحيح موجب.

229. إذا كان $n \le 5$ فإن المعادلة $(n-1)!+1 = n^2$ متحققة عندما $n = 5$. لنفرض أن $n \ge 6$. لنكتب المعادلة على الشكل $(n-1)! = n^2 - 1$. بالتبسيط نحصل على $(n-2)! = n+1$. لكن بما أن $n \ge 6$ فإن $(n-2)! > 2(n-2) > n+1$. هذا يقتضي أن المعادلة $(n-1)!+1 = n^2$ غير متحققة للقيم $n \ge 6$. إذاً للمعادلة المعطاة حل وحيد هو $n = 5$.

230. بفرض وجود عددين صحيحين موجبين c و d يقسمان b و $c + d \equiv 0 \bmod a$ يمكننا أن نكتب $b = cc'$ و $b = dd'$ و $c + d = ka$، حيث c'، d'، k أعداد صحيحة موجبة. هذا يعطينا

$$\frac{a}{b} = \frac{ka}{kb} = \frac{c+d}{kb} = \frac{1}{kc'} + \frac{1}{kd'}$$

ومنه نستنتج أن $(x,y) = (kc',kd')$ هو حل للمعادلة المعطاة.

الآن نفرض أن المعادلة المعطاة قابلة للحل وليكن (x,y) هو أحد الحلول الصحيحة الموجبة. نكتب المعادلة على الصورة

$$axy = b(x+y)$$

لنضع $g = (x,y)$. إذاً $x = cg$ و $y = dg$ حيث c و d عددان صحيحان موجبان و $(c,d) = 1$. المعادلة السابقة تصبح

$$agdc = b(c+d)$$

حيث إنَّ $(c,d)=1$ فإن $(c,c+d)=1$ ومنه نستنتج من المعادلة السابقة أن $b \mid c$. وبطريقة مشابهة يصبح لدينا $b \mid d$ أيضاً. و حيث إنَّ $(a,b)=1$ فإن a يقسم $c+d$، أي أن $c+d \equiv 0 \bmod a$.

231. نلاحظ أولاً أن x و y لا يمكن أن يكون كلاهما سالباً. نبدأ بافتراض $|y| \le |x|$. المعادلة يمكن كتابتها على الشكل

$$6x+6y=5xy \text{ ....(*)}$$

هذا يقتضي أن

$$|5xy|=|6x+6y| \le |6x|+|6y| \le |12y|$$

ومن ثم $|x| \le 12/5$ (لأن $y \neq 0$). إذاً $x=\pm 1, \pm 2$. بتعويض هذه القيم في المعادلة (*) نحصل على الحلول $(x,y)=(1,-6), (2,3)$. وبنفس الطريقة، عند افتراض $|x| \le |y|$، نحصل على الحلول $(x,y)=(-6,1), (3,2)$. إذاً حلول المعادلة المعطاة هي

$$(x,y)=(1,-6),\ (-6,1),\ (2,3),\ (3,2)$$

232. من المعادلة $x^2y^2+x^2y+xy^2+xy=xyz-1$ نستنتج أن $xy \mid 1$ ومن ثم

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

بالتعويض عن هذه القيم في المعادلة الأصلية نحصل على القيمة المقابلة للمتغير z. الحلول هي

$$(x,y,z)=(1,1,5),\ (1,-1,-1),\ (-1,1,-1),\ (-1,-1,1)$$

233. من المعادلة $2xy+3y^2=24$ نستنتج أن y عدد زوجي. بكتابة $y=2w$، المعادلة تصبح

$$xw+3w^2=6$$

هذا يقتضي أن $w\mid 6$ ومن ثم $w=\pm1,\ \pm2,\ \pm3,\ \pm6$. بالتعويض في المعادلة السابقة نحصل على التوالي $x=\pm3,\ \mp3,\ \mp7,\ \mp17$. بما أن $y=2w$، إذاً للمعادلة الأصلية ثمانية حلول هي

$$(x,y)=(\pm3,\pm2),\ (\mp3,\pm4),\ (\mp7,\pm6),\ (\mp17,\pm12)$$

234. إذا كان $n\le3$ نجد بسهولة أن $(n,m)=(2,1)$ هو الحل الوحيد للمعادلة

$$1!+2!+3!+\cdots+n!=m^2+2$$

لنفرض الآن أن $n\ge4$. بحساب المعادلة قياس 4 نحصل على التطابق

$$1!+2!+3!\equiv m^2+2 \bmod 4$$

أو بالتبسيط $m^2\equiv3 \bmod 4$، و هو تطابق غير قابل للحل. هذا يعني أنه لا يوجد حل للمعادلة المعطاة عندما $n\ge4$. نستنتج أن $(n,m)=(2,1)$ هو الحل الوحيد للمعادلة.

235. إذا كانت المعادلة المعطاة قابلة للحل، فإن التطابق

$$x^6+3\equiv y^3+z^3 \bmod 7$$

قابل أيضاً للحل. بما أن $a^3\equiv0,1,-1 \bmod 7$ وبواسطة نظرية فيرما $x^6\equiv0,1 \bmod 7$، نلاحظ أن $y^3+z^3\equiv0,1,2,-1,-2 \bmod 7$ و

$x^6+3\equiv 3,4 \bmod 7$. بدراسة جميع الاحتمالات، نلاحظ أن $x^6+3\not\equiv y^3+z^3 \bmod 7$. هذا يعني أنه لا توجد حلول صحيحة للمعادلة $x^6+3=y^3+z^3$.

236. بحساب المعادلة $2x^3+x^2+5y+7=0$ قياس 5 نحصل على التطابق $2x^3+x^2+2\equiv 0 \bmod 5$ والذي يوجد له حلان هما $x\equiv 1 \bmod 5$ و $x\equiv -2 \bmod 5$. عند كتابة الحلين على الصورة $x=1+5t$ و $x=-2+5t$ ومن ثم التعويض عن x في المعادلة الأصلية نحصل على قيمة y. الحلول معطاة كالتالي:

$$\begin{aligned}(x,y)=&(1+5t,-50t^3-35t^2-8t-2),\\ &(-2+5t,-50t^3+55t^2-20t+1)\end{aligned}$$

حيث t عدد صحيح.

237. نضرب أولاً طرفي المعادلة $4x^4-2=y(y+1)$ بالعدد 4، ثم نقوم بإكمال المربع في المتغير y لنحصل على المعادلة $16x^4-7=(2y+1)^2$، والتي يمكن كتابتها على الصورة $(4x^2)^2-(2y+1)^2=7$. بالتحليل يصبح لدينا $(4x^2-2y-1)(4x^2+2y+1)=7$. هذا بدوره يعطينا الاحتمالات الآتية:

$$\begin{cases}4x^2-2y-1=\pm 1,\ \pm 7\\ 4x^2+2y+1=\pm 7,\ \pm 1\end{cases}$$

بحل الأنظمة أعلاه، نجد أن $(x,y)=(1,1),\ (1,-2),\ (-1,1),\ (-1,-2)$ هي الحلول الوحيدة للمعادلة $4x^4-2=y(y+1)$.

238. بضرب طرفي المعادلة $x + y = x^2 + y^2$ بالعدد 4، ومن ثم إكمال المربع في المتغيرين x و y نحصل على المعادلة $(2x-1)^2 + (2y-1)^2 = 2$. هذا يعطينا الاحتمالات الآتية:

$$\begin{cases} 2x-1=\pm 1, & \pm 1 \\ 2y-1=\pm 1, & \mp 1 \end{cases}$$

ينتج من ذلك الحلول الأربعة:

$$(x,y)=(0,0),\ (0,1),\ (1,0),\ (1,1).$$

239. بضرب المعادلة $2xy+5x+7y=3$ بالعدد 2 ومن ثم إضافة 35 للطرفين نحصل على المعادلة

$$4xy+10x+14y+35=41$$

بالتحليل يصبح لدينا المعادلة $(2x+7)(2y+5)=41$ ومن ثم

$$\begin{cases} 2x+7=\pm 1, & \pm 41 \\ 2y+5=\pm 41, & \pm 1 \end{cases}$$

هذا يُعطينا الحلول:

$$(x,y)=(-3,18),\ (-4,-23),\ (17,-2),\ (-24,-3).$$

240. نبدأ الحل بافتراض أن $x \le y \le z \le w$ (لأن تغيير ترتيب المتغيرات لن يغير من جوهر المعادلة الأصلية.) إذا كان $x=1$ فإن المعادلة تصبح $0=\frac{1}{y^2}+\frac{1}{z^2}+\frac{1}{w^2}$، وهذا مستحيل. إذاً لابد أن يكون $x \ge 2$، ومن ثم $y \ge 2$ و $z \ge 2$ و $w \ge 2$. لكن إذا كان $w \ge 3$ فسوف يصبح

لدينا

$$1=\frac{1}{x^2}+\frac{1}{y^2}+\frac{1}{z^2}+\frac{1}{w^2}\le\frac{1}{4}+\frac{1}{4}+\frac{1}{4}+\frac{1}{9}=\frac{31}{36}<1$$

وهذا مستحيل. إذاً لابد أن يكون $w \le 2$. هذا يقتضي أن

$$2\le x \le y \le z \le w \le 2$$

ومنه نستنتج أن $x=y=z=w=2$، أي أن $(x,y,z,w)=(2,2,2,2)$ هو الحل الوحيد للمعادلة المعطاة.

241. نبدأ الحل بفرض أن $x \le y$. بما أن $x!+y!=z!$ فإن $y!<z!$ ومن ثم $y<z$. هذا يقتضي أن $z \ge y+1$ ومن ثم

$$z!\ge(y+1)!$$

أيضاً بما أن $x \le y$ فإن

$$z!=x!+y!\le y!+y!=2(y!)$$

من المتباينتين السابقتين نستنتج أن $(y+1)!\le 2(y!)$. هذا يقتضي أن $y+1\le 2$ ومن ثم $y=1$ لأن y عدد صحيح موجب. بسبب الفرض $x\le y$ نستنتج أن $x=1$. هذا يقتضي أن $z=2$.

عندما نفرض أن $y\le x$ فإننا سوف نحصل على نفس الحل. إذاً للمعادلة المعطاة حلٌ وحيد هو $(x,y,z)=(1,1,2)$.

242. بما أن المتغيرات n,x,y,z هي أعداد صحيحة موجبة فنستنتج من المعادلة $n^x+n^y=n^z$ أن n عدد زوجي (وإلا فسوف نحصل على عدد فردي = عدد زوجي). أيضاً بما أن $n^z>n^x$ و $n^z>n^y$

فإن $x > z$ و $y > z$. لأن استبدال موقع المتغيرين x و y ببعضهما لن يغير من جوهر المعادلة، فيمكننا أن نفرض أن $x \le y$. هذا يقتضي أن $n^z = n^x + n^y \le n^y + n^y = 2n^y$ أو $n^{z-y} \le 2$. نستنتج من ذلك أنه إما $n^{z-y} = 1$ أو $n^{z-y} = 2$. الحالة الأولى تقتضي أن $n = 1$ وهذا مُستحيل. الحالة الثانية تقتضي أن $n = 2$ و $z - y = 1$. هذا يُعطينا $2^x + 2^y = 2^{y+1}$، أو $2^x = 2^{y+1} - 2^y = 2^y$ ومن ثم $x = y$. إذاً حلول المعادلة هي $(n, x, y, z) = (2, t, t, t+1)$ حيث t عدد صحيح موجب.

243. لاحظ أولاً أنَّ $3^2 + 4^2 = 5^2$. لنفرض أنَّ $n \ge 3$. في هذه الحالة نحصل على الآتي:

$$5^n = 5^2 \times 5^{n-2} = (3^2 + 4^2) \times 5^{n-2} = 3^2 \times 5^{n-2} + 4^2 \times 5^{n-2}$$
$$> 3^2 \times 3^{n-2} + 4^2 \times 4^{n-2} = 3^n + 4^n$$

أي أن $3^n + 4^n \ne 5^n$ إذا كان $n \ge 3$. نستنتج من ذلك أن المعادلة $3^n + 4^n = 5^n$ ليس لها أي حلٍ صحيح $n \ge 3$.

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

245. إذا كان $x = 0$ أو $y = 0$ نحصل على حلٍ وحيد هو $(x, y) = (3, 0)$ للمعادلة $2^x - 3^y = 7$. لنفرض أنَّ $x \ge 1$ و $y \ge 1$. بحساب المعادلة قياس 3 نحصل على التطابق $2^x \equiv 1 \bmod 3$ ومنه

نستنتج أن x عدد زوجي ($x \geq 2$). وبحساب المعادلة قياس 4 نحصل على التطابق $(-1)^y \equiv 1 \bmod 4$ ومنه نستنتج أن y عدد زوجي. هذا يُمكننا من كتابة المعادلة على الشكل الآتي:

$$(2^{x/2} - 3^{y/2})(2^{x/2} + 3^{y/2}) = 7$$

حيث إنَّ العدد 7 عدد أولي و $2^{x/2} + 3^{y/2} > 1$، إذاً نحصل على المعادلة

$$2^{x/2} - 3^{y/2} = 1$$

باستخدام مثال 68 نجد أن $x/2 = 2$ و $y/2 = 1$، أي أن $x = 4$ و $y = 2$. إذاً يوجد للمعادلة المعطاة حلان هما $(x, y) = (3,0), \ (4,2)$.

246. إذا كان $n = 1$ فإن $(n, x, m) = (1, 1, t)$، حيث t عدد صحيح موجب، هو حل للمعادلة

$$2^n - x^m = 1$$

أيضاً إذا كان $m = 1$ فإن $(n, x, m) = (t, 2^t - 1, 1)$، حيث t عدد صحيح موجب، هو حلٌ للمعادلة المُعطاة. لنفرض الآن أنه توجد حلول صحيحة عندما $n > 1$ و $m > 1$. بحساب المعادلة أعلاه قياس 4، نستنتج أن التطابق $x^m \equiv 3 \bmod 4$ قابل للحل. في هذه الحالة لابد أن يكون x عدداً فردياً. لنكتب $x = 2a + 1$. بملاحظة أن

$$(2a+1)^m = \sum_{j=0}^{m} \binom{m}{j} (2a)^j \equiv 1 + 2ma \bmod 4$$

نستنتج أن $x^m \equiv 3 \bmod 4$ إذا وفقط إذا كان $1 + 2ma \equiv 3 \bmod 4$، أي أن $ma \equiv 1 \bmod 2$. هذا يقتضي أن m عدد فردي. بكتابة المعادلة

الأصلية على الصورة

$$2^n = (x+1)(x^{m-1} - x^{m-2} + \cdots - x + 1)$$

ينتج لدينا تناقض لأن $x^{m-1} - x^{m-2} + \cdots - x + 1$ عدد فردي (لأن x و m عددين فرديين) لا يساوي 1. إذاً لا توجد حلول صحيحة للمعادلة المعطاة عندما $n > 1$ و $m > 1$. لذا فالحلول الوحيدة للمعادلة هي $(n, x, m) = (1,1,t),\ (t, 2^t - 1, 1)$ حيث t عدد صحيح موجب.

247. إذا كان x عدداً زوجياً فإن $2^x + 5^y \equiv 1 + (-1)^y \not\equiv 1 \bmod 3$، بينما $19^z \equiv 1^z \equiv 1 \bmod 3$. هذا يعني أنه ليس للمعادلة $2^x + 5^y = 19^z$ حلاً إذا كان x عدداً زوجياً.

إذا كان $x = 2n + 1$ عدداً فردياً فإن $2^x + 5^y = 2 \times 4^n + 5^y \equiv 2 \times (-1)^n \bmod 5$، بينما $19^z \equiv (-1)^z \bmod 5$. هذا يعني أن $2^x + 5^y \not\equiv 19^z \bmod 5$ ومن ثم فالمعادلة $2^x + 5^y = 19^z$ ليس لها أي حل إذا كان x عدداً فردياً. نستنتج من ذلك أن المعادلة $2^x + 5^y = 19^z$ ليس لها أي حل صحيح موجب.

248. لنفرض أن (x_0, y_0) هو حل للمعادلة $y^2 = x^3 - 3$. إذا كان x_0 عدداً زوجياً فسوف نحصل على التطابق $y_0^2 \equiv 0 - 3 \equiv 5 \bmod 8$، وهذا مستحيل لأن $a^2 \equiv 0,1,4 \bmod 8$ لأي عدد صحيح a. إذاً لابُد أن يكون x_0 عدداً فردياً، أي أنه إما $x_0 \equiv 1 \bmod 4$ أو $x_0 \equiv 3 \bmod 4$.

لِنفرض أن $x_0 \equiv 1 \bmod 4$. لِنكتب المعادلة على الشكل الآتي:

$$y_0^2 + 4 = x_0^3 + 1 = (x_0 + 1)(x_0^2 - x_0 + 1)$$

بما أن $x_0 \equiv 1 \bmod 4$ فإن $x_0 + 1 \equiv 2 \bmod 4$، أي أن $2 \| x_0 + 1$. هذا يقتضي أن $2 \| x_0^3 + 1$ لأن $x_0^2 - x_0 + 1$ عدد فردي. لكن $4 | y_0^2 + 4$ (لأن y_0 عدد زوجي إذا كان x_0 فردي.) هذا التناقض يُثبِت أن $x_0 \not\equiv 1 \bmod 4$.

إذا كان $x_0 \equiv 3 \bmod 4$ فإن $x_0^2 - x_0 + 1 \equiv 3 \bmod 4$ ومن ثم فإن المقدار $x_0^2 - x_0 + 1$ يقبل القسمة على عدد أولي p يُحقِق $p \equiv 3 \bmod 4$. هذا يقتضي أن $y_0^2 + 4 \equiv 0 \bmod p$، أي أن $y_0^2 \equiv -4 \bmod p$. هذا يُعطينا

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

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

249. لنفرض أن (x_0, y_0) هو حل للمعادلة $y^2 = x^3 - 12$. إذا كان x_0 عدداً زوجياً فإن y_0 عدد زوجي أيضاً. بكتابة $x_0 = 2x_1$ و $y_0 = 2y_1$ و بالتعويض في المعادلة أعلاه نحصل على المعادلة $y_1^2 = 2x_1^3 - 3$. هذا يقتضي أن y_1 عدد فردي ومن ثم x_1 عدد زوجي ($y_1 = 2k + 1$ يقتضي أن $2x_1^3 = y_1^2 + 3 = 4k^2 + 4k + 4$ أو $x_1^3 = 2k^2 + 2k + 2$، أي أن x_1 عدد زوجي). بحساب المعادلة $y_1^2 = 2x_1^3 - 3$ قياس 8 نحصل على $1 \equiv 0 - 3 \bmod 8$ وهذا مستحيل.

نفرض الآن أن x_0 عدد فردي. هذا يقتضي أن y_0 عدد فردي أيضاً. لنكتب المعادلة المعطاة على الصورة

$$y_0^2 + 4 = x_0^3 - 8 = (x_0 - 2)(x_0^2 + 2x_0 + 4)$$

بما أن $x_0 = 2k + 1$ فإن $x_0^2 + 2x_0 + 4 = 4t + 3$. هذا يقتضي أن $x_0^2 + 2x_0 + 4$ يقبل القسمة على عدد أولي p يُحقق $p \equiv 3 \bmod 4$. هذا يقتضي أن $y_0^2 + 4 \equiv 0 \bmod 4$ وهذا مستحيل (كما في السؤال السابق). نستنتج من ذلك أنه لا يوجد أي حل صحيح للمعادلة المعطاة.

250. لِنفرض أن (x, y) هو حلٌ صحيحٌ للمعادلة $y^2 = x^3 + 16$. إذا كان y عدداً فردياً فإن $(y - 4, y + 4) = 1$. بكتابة المعادلة على الصورة

$$(y - 4)(y + 4) = x^3$$

نستنتج أنه يوجد عددان صحيحان a و b يُحقِقان

$$y - 4 = a^3, \quad y + 4 = b^3$$

هذا يقتضي أن $b^3 - a^3 = 8$ والتي ليس لها حلول صحيحة (باستخدام طريقة التحليل). إذاً y لا يمكن أن يكون عدداً فردياً.

لِنفرض أن y عدد زوجي. هذا يقتضي أن x عدد زوجي أيضاً. بكتابة $y = 2y_1$ و $x = 2x_1$ ومن ثم التعويض في المعادلة الأصلية نحصل على المعادلة $y_1^2 = 2x_1^3 + 4$. هذا يقتضي أن y_1 عدد زوجي، و ليكن $y_1 = 2y_2$. بالتعويض في المعادلة السابقة نحصل على المعادلة $2y_2^2 = x_1^3 + 2$ ومن ثم x_1 عدد زوجي، وليكن $x_1 = 2x_2$. بالتعويض نحصل على المعادلة $y_2^2 = 4x_2^3 + 1$. هذا يقتضي أن y_2 عدد فردي، وليكن $y_2 = 2y_3 + 1$. هذا يؤدي إلى المعادلة $4y_3^2 + 4y_3 + 1 = 4x_2^3 + 1$ أو

$$y_3(y_3 + 1) = x_2^3$$

حيث إنَّ $(y_3, y_3+1)=1$ فإنه يوجد عددان صحيحان c و d يُحققان

$$y_3 = c^3, \quad y_3+1 = d^3$$

هــذا يعطــي المعادلــة $d^3 - c^3 = 1$ والتــي لهــا حــلان همــا $(c,d)=(0,1),\ (-1,0)$، باستخدام طريقة التحليل. هذا يقتضي الآتي:

$$c=0 \Rightarrow y_3=0 \Rightarrow y_2=1 \Rightarrow y_1=2 \Rightarrow y=4 \Rightarrow x=0$$

$$c=-1 \Rightarrow y_3=-1 \Rightarrow y_2=-1 \Rightarrow y_1=-2 \Rightarrow y=-4 \Rightarrow x=0$$

أي أن للمعادلــة $y^2 = x^3 + 16$ حلــين صــحيحين همــا $(x,y)=(0,-4),\ (0,4)$.

كشاف مواضيع المسائل

الأعداد الأولية الأقل من 5000

2	109	269	439	617	811	1009	1201
3	113	271	443	619	821	1013	1213
5	127	277	449	631	823	1019	1217
7	131	281	457	641	827	1021	1223
11	137	283	461	643	829	1031	1229
13	139	293	463	647	839	1033	1231
17	149	307	467	653	853	1039	1237
19	151	311	479	659	857	1049	1249
23	157	313	487	661	859	1051	1259
29	163	317	491	673	863	1061	1277
31	167	331	499	677	877	1063	1279
37	173	337	503	683	881	1069	1283
41	179	347	509	691	883	1087	1289
43	181	349	521	701	887	1091	1291
47	191	353	523	709	907	1093	1297
53	193	359	541	719	911	1097	1301
59	197	367	547	727	919	1103	1303
61	199	373	557	733	929	1109	1307
67	211	379	563	739	937	1117	1319
71	223	383	569	743	941	1123	1321
73	227	389	571	751	947	1129	1327
79	229	397	577	757	953	1151	1361
83	233	401	587	761	967	1153	1367
89	239	409	593	769	971	1163	1373
97	241	419	599	773	977	1171	1381
101	251	421	601	787	983	1181	1399
103	257	431	607	797	991	1187	1409
107	263	433	613	809	997	1193	1423

1427	1619	1873	2111	2351	2609	2801	3049
1429	1621	1877	2113	2357	2617	2803	3061
1433	1627	1879	2129	2371	2621	2819	3067
1439	1637	1889	2131	2377	2633	2833	3079
1447	1657	1901	2137	2381	2647	2837	3083
1451	1663	1907	2141	2383	2657	2843	3089
1453	1667	1913	2143	2389	2659	2851	3109
1459	1669	1931	2153	2393	2663	2857	3119
1471	1693	1933	2161	2399	2671	2861	3121
1481	1697	1949	2179	2411	2677	2879	3137
1483	1699	1951	2203	2417	2683	2887	3163
1487	1709	1973	2207	2423	2687	2897	3167
1489	1721	1979	2213	2437	2689	2903	3169
1493	1723	1987	2221	2441	2693	2909	3181
1499	1733	1993	2237	2447	2699	2917	3187
1511	1741	1997	2239	2459	2707	2927	3191
1523	1747	1999	2243	2467	2711	2939	3203
1531	1753	2003	2251	2473	2713	2953	3209
1543	1759	2011	2267	2477	2719	2957	3217
1549	1777	2017	2269	2503	2729	2963	3221
1553	1783	2027	2273	2521	2731	2969	3229
1559	1787	2029	2281	2531	2741	2971	3251
1567	1789	2039	2287	2539	2749	2999	3253
1571	1801	2053	2293	2543	2753	3001	3257
1579	1811	2063	2297	2549	2767	3011	3259
1583	1823	2069	2309	2551	2777	3019	3271
1597	1831	2081	2311	2557	2789	3023	3299
1601	1847	2083	2333	2579	2791	3037	3301
1607	1861	2087	2339	2591	2797	3041	3307
1609	1867	2089	2341	2593			
1613	1871	2099	2347				

3313	3527	3709	3923	4139	4363	4597	4813
3319	3529	3719	3929	4153	4373	4603	4817
3323	3533	3727	3931	4157	4391	4621	4831
3329	3539	3733	3943	4159	4397	4637	4861
3331	3541	3739	3947	4177	4409	4639	4871
3343	3547	3761	3967	4201	4421	4643	4877
3347	3557	3767	3989	4211	4423	4649	4889
3359	3559	3769	4001	4217	4441	4651	4903
3361	3571	3779	4003	4219	4447	4657	4909
3371	3581	3793	4007	4229	4451	4663	4919
3373	3583	3797	4013	4231	4457	4673	4931
3389	3593	3803	4019	4241	4463	4679	4933
3391	3607	3821	4021	4243	4481	4691	4937
3407	3613	3823	4027	4253	4483	4703	4943
3413	3617	3833	4049	4259	4493	4721	4951
3433	3623	3847	4051	4261	4507	4723	4957
3449	3631	3851	4057	4271	4513	4729	4967
3457	3637	3853	4073	4273	4517	4733	4969
3461	3643	3863	4079	4283	4519	4751	4973
3463	3659	3877	4091	4289	4523	4759	4987
3467	3671	3881	4093	4297	4547	4783	4993
3469	3673	3889	4099	4327	4549	4787	4999
3491	3677	3907	4111	4337	4561	4789	
3499	3691	3911	4127	4339	4567	4793	
3511	3697	3917	4129	4349	4583	4799	
3517	3701	3919	4133	4357	4591	4801	

المراجـع

المراجع العربية

[1] مقدمة في نظرية الأعداد، د. فوزي الذكير و د. معروف سمحان، الطبعة الثانية، دار الخريجي للنشر و التوزيع، الرياض، 1422 هـ.

المراجع الأجنبية

[2] Adams, W.W. and Goldstein, L. J., Introduction to Number Theory, Prentice-Hall, New Jersey, 1976.

[3] Andrews, George E., Number Theory, Dover Publications, New York, 1994.

[4] Burton, David M., Elementary Number Theory, 6th edition, McGraw-Hill, New York, 2007.

[5] Davenport, H., The Higher Arithmetic, 7th edition, Cambridge University Press, Cambridge, 1999.

[6] Dudley, Underwood, Elementary Number Theory, W. H. Freeman & Company, San Francisco, 1969.

[7] Elliot, D. D., A Prime-Generating Function, The Two-Year College Math. Journal, 14 (1983), 57.

[8] Giblin, Peter, Primes and Programming, Cambridge University Press, Cambridge, 1993.

[9] Gioia, Anthony A., The Theory of Numbers: An Introduction, Dover Publications, New York, 2001.

[10] Gross, Oliver, On the Elementary Approach to Diophantine Equations, Math. Magazine, 34 (1961), 259-267.

[11] Guy, Richard K., Unsolved Problems in Number Theory, 2nd edition, Springer, New York, 1994.

[12] Herman, J., Kucera, R., and Simsa, J., Equations and Inequalities, Springer, New York, 2000.

[13] Jones, Burton W., The Theory of Numbers, Holt, Rinehart and Winston, New York, 1966.

[14] Krizik, M., Luca, F., and Somer, L., 17 Lectures on Fermat Numbers, Springer, New York, 2001.

[15] Kumanduri, R. and Romero C., Number Theory with Computer Applications, Prentice-Hall, New Jersey, 1998.

[16] LeVeque, Williams J., Fundamentals of Number Theory, Dover Publications, Inc., New York, 1996.

[17] Mollin, Richard A., Fundamental Number Theory with Applications, CRC Press, Boca Raton, 1998.

[18] Nagell, Trygve, Introduction to Number Theory, Chelsea Publishing Company, New York, 1981.

[19] Narkiewicz, W., The Development of Prime Number Theory, Springer, Berlin, 2000.

[20] Nathanson, Melvyn B., Elementary Methods in Number Theory, GTM 195, Springer, New York, 2000.

[21] Niven, I., Zuckerman, H., and Montgomery, H., An Introduction to the Theory of Numbers, 5th edition, John Wiley & Sons, New York, 1991.

[22] Ore, Oystein, Number Theory and its History, Dover Publications, New York, 1988.

[23] Redmond, Don, Number Theory: An Introduction, Marcel Dekker, New York, 1996.

[24] Roberts, Joe, Elementary Number Theory: A Problem Oriented Approach, MIT Press, Cambridge, 1977.

[25] Ribenboim, Paulo, Fermat's Last Theorem for Amateurs, Springer-Verlag, New York, 1999.

[26] Shapiro, Harold N., Introduction to the Theory of Numbers, John Wiley & Sons, New York, 1983.

[27] Shockley, James, Introduction to Number Theory, Holt, Rinehart and Winston, Inc., New York, 1967.

[28] Stark, Harold M., An Introduction to Number Theory, MIT Press, Cambridge, 10th printing, 1998.

[29] Stewart, B. M., Theory of Numbers, 2nd edition, Macmillan Company, New York, 1964.

[30] Tattersall, James T., Elementary Number Theory in Nine Chapters, Cambridge University Press, Cambridge, 1999.

[31] Uspencky, J. V. and Heaslet, M., Elementary Number Theory, McGraw-Hill Book Company, Inc., New York, 1939.

[32] Vinogradov, I. M., An Introduction to the Theory of Numbers, Pergamon Press, New York, 1955.

[33] Williams, Kenneth S. and Hardy, Kenneth, The Red Book of Mathematical Problems, Dover Publications, New York, 1996.