Problema plantejat a la secció “Divertiments” d’El Full d’Abril 2008

Si p i q són dos primers tals que $p > q > 3$, proveu que $p^2 - q^2$ és múltiple de 24.

Resolució:

S’hi aporten tres demostracions.

◆ Demostració 1

Pel que es refereix a q, d’una banda:

$$\left.\begin{array}{c} q \text{ primer} \\ \wedge \\ q > 3 \end{array}\right\} \Rightarrow q \neq \dot{3} \Rightarrow \left\{\begin{array}{c} q \equiv 1 (\text{mod } 3) \\ \vee \\ q \equiv 2 (\text{mod } 3) \end{array}\right. \Rightarrow \left\{\begin{array}{c} q^2 \equiv 1 (\text{mod } 3) \\ \vee \\ q^2 \equiv 4 (\text{mod } 3) \end{array}\right. \overset{(*)}{\Rightarrow} q^2 \equiv 1 (\text{mod } 3) \quad (1)$$

$^{(*)}\ 4 \equiv 1 (\text{mod } 3)$

I d’altra banda:

$$\left.\begin{array}{c} q \text{ primer} \\ \wedge \\ q > 3 \end{array}\right\} \Rightarrow q \text{ senar} \Rightarrow \left\{\begin{array}{c} q \equiv 1 (\text{mod } 8) \\ \vee \\ q \equiv 3 (\text{mod } 8) \\ \vee \\ q \equiv 5 (\text{mod } 8) \\ \vee \\ q \equiv 7 (\text{mod } 8) \end{array}\right. \Rightarrow \left\{\begin{array}{c} q^2 \equiv 1 (\text{mod } 8) \\ \vee \\ q^2 \equiv 9 (\text{mod } 8) \\ \vee \\ q^2 \equiv 25 (\text{mod } 8) \\ \vee \\ q^2 \equiv 49 (\text{mod } 8) \end{array}\right. \overset{(**)}{\Rightarrow} q^2 \equiv 1 (\text{mod } 8) \quad (2)$$

$^{(**)}\ 9 \equiv 1 (\text{mod } 8),\ 25 \equiv 1 (\text{mod } 8),\ 49 \equiv 1 (\text{mod } 8)$

Com que 3 i 8 són primers entre si:

$$\left.\begin{array}{c} (1) \\ \wedge \\ (2) \end{array}\right\} \Rightarrow q^2 \equiv 1 (\text{mod } 24) \quad (a)$$

Quant a p:

$$\left.\begin{array}{c} p \text{ primer} \\ \wedge \\ p > q > 3 \end{array}\right\} \Rightarrow \left\{\begin{array}{l} p \neq \dot{3} \\ \wedge \\ p \text{ senar} \end{array}\right. \Rightarrow \cdots \Rightarrow p^2 \equiv 1 (\text{mod } 24) \quad (b)$$

Així doncs, en relació a $p^2 - q^2 \,(> 0)$ es pot concloure que:

$$\left.\begin{array}{c} (a) \\ \wedge \\ (b) \end{array}\right\} \Rightarrow p^2 - q^2 \equiv 0 (\text{mod } 24) \Rightarrow 24 \mid (p^2 - q^2) \Rightarrow \boxed{p^2 - q^2 = \dot{24}}$$

◆ Demostració 2

Pel que es refereix a q :

$$q^2-1=(q-1)(q+1)$$

A més, d'una banda:

$$\left.\begin{array}{c} q\in\mathbb{Z} \\ \wedge \\ q>3 \end{array}\right\} \Rightarrow \begin{cases} q=3k+1 \\ \vee \\ q=3k+2 \\ \vee \\ q=3k+3=3(k+1) \\ (k=1,2,3,\ldots) \end{cases}$$

I com que $(q \text{ primer}) \wedge (q>3) \Rightarrow q \neq \dot{3}$, llavors:

$$q\neq\dot{3} \Rightarrow \begin{cases} q=3k+1 \\ \vee \\ q=3k+2 \\ (k=1,2,3,\ldots) \end{cases} \Rightarrow \begin{cases} (q-1=3k)\wedge(q+1=3k+2) \\ \vee \\ (q-1=3k+1)\wedge(q+1=3(k+1)) \\ (k=1,2,3,\ldots) \end{cases} \Rightarrow \begin{cases} 3\mid(q-1) \\ \vee \\ 3\mid(q+1) \end{cases} \Rightarrow 3\mid(q^2-1) \quad (1)$$

D'altra banda:

$$\left.\begin{array}{c} q\in\mathbb{Z} \\ \wedge \\ q>3 \end{array}\right\} \Rightarrow \begin{cases} q=2n \\ \vee \\ q=2n+1 \\ (n=2,3,4,\ldots) \end{cases}$$

I com que $(q \text{ primer}) \wedge (q>3) \Rightarrow q$ senar , llavors:

$$q \text{ senar} \Rightarrow \begin{array}{c} q=2n+1 \\ (n=2,3,4,\ldots) \end{array} \Rightarrow \begin{cases} q-1=2n \\ \wedge \\ q+1=2(n+1) \\ (n=2,3,4,\ldots) \end{cases} \overset{(*)}{\Rightarrow} \begin{cases} (4\mid(q-1))\wedge(2\mid(q+1)) \\ \vee \\ (2\mid(q-1))\wedge(4\mid(q+1)) \end{cases} \Rightarrow 8\mid(q^2-1) \quad (2)$$

$^{(*)}$ $n,\ n+1$ consecutius $\forall n\in\{2,3,4,\ldots\} \Rightarrow \begin{cases} n=2m \\ \vee \\ n+1=2m \\ (m\in\{1,2,3,\ldots\}) \end{cases}$

Per tant:

$$\left.\begin{array}{c} (1) \\ \wedge \\ (2) \end{array}\right\} \Rightarrow 24\mid(q^2-1) \quad (a)$$

Quant a p :

$$p^2-1=(p-1)(p+1)$$

I llavors:

$$\left.\begin{array}{c} p \text{ primer} \\ \wedge \\ p>q>3 \end{array}\right\} \Rightarrow \left\{\begin{array}{c} p \neq \dot{3} \\ \wedge \\ p \text{ senar} \end{array}\right. \Rightarrow \cdots \Rightarrow 24 \mid (p^2-1) \quad \text{(b)}$$

Així doncs, en relació a $p^2-q^2\,(>0)$ es pot concloure que:

$$\left.\begin{array}{c} \text{(a)} \\ \wedge \\ \text{(b)} \end{array}\right\} \Rightarrow 24 \mid ((p^2-1)-(q^2-1)) \Rightarrow 24 \mid (p^2-q^2) \Rightarrow \boxed{p^2-q^2=\dot{24}}$$

◆ <u>Demostració 3</u>

Pel que es refereix a q :

$$q^2-1=(q-1)(q+1)$$

A més:

$$\left.\begin{array}{c} q \in \mathbb{Z} \\ \wedge \\ q>3 \end{array}\right\} \Rightarrow \left\{\begin{array}{c} q=6k-2=2(3k-1) \\ \vee \\ q=6k-1 \\ \vee \\ q=6k=2(3k) \\ \vee \\ q=6k+1 \\ \vee \\ q=6k+2=2(3k+1) \\ \vee \\ q=6k+3=3(2k+1) \\ (k=1,2,3,\ldots) \end{array}\right.$$

I com que $(q \text{ primer}) \wedge (q>3) \Rightarrow (q \neq \dot{3}) \wedge (q \text{ senar})$, llavors:

$$\left\{\begin{array}{c} q \neq \dot{3} \\ \wedge \\ q \text{ senar} \end{array}\right. \Rightarrow \left\{\begin{array}{c} q=6k-1 \\ \vee \\ q=6k+1 \\ (k=1,2,3,\ldots) \end{array}\right. \Rightarrow \left\{\begin{array}{c} (q-1=2(3k-1)) \wedge (q+1=2(3k)) \\ \vee \\ (q-1=2(3k)) \wedge (q+1=2(3k+1)) \\ (k=1,2,3,\ldots) \end{array}\right. \Rightarrow \left\{\begin{array}{c} q^2-1=12k(3k-1) \\ \vee \\ q^2-1=12k(3k+1) \\ (k=1,2,3,\ldots) \end{array}\right.$$

Quan $k=1,3,5,\ldots$:

$$\begin{cases} q^2-1=12(2n-1)(3(2n-1)-1) \\ \vee \\ q^2-1=12(2n-1)(3(2n-1)+1) \\ (n=1,2,3,\ldots) \end{cases} \Rightarrow \begin{cases} q^2-1=24(2n-1)(3n-2) \\ \vee \\ q^2-1=24(2n-1)(3n-1) \\ (n=1,2,3,\ldots) \end{cases} \Rightarrow 24 \mid (q^2-1) \quad (1)$$

I quan $k=2,4,6,\ldots$:

$$\begin{cases} q^2-1=12(2n)(3(2n)-1) \\ \vee \\ q^2-1=12(2n)(3(2n)+1) \\ (n=1,2,3,\ldots) \end{cases} \Rightarrow \begin{cases} q^2-1=24n(6n-1) \\ \vee \\ q^2-1=24n(6n+1) \\ (n=1,2,3,\ldots) \end{cases} \Rightarrow 24 \mid (q^2-1) \quad (2)$$

Per tant:

$$\left.\begin{matrix} (1) \\ \wedge \\ (2) \end{matrix}\right\} \Rightarrow 24 \mid (q^2-1) \quad (a)$$

Quant a p:

$$p^2-1=(p-1)(p+1)$$

I llavors:

$$\left.\begin{matrix} p \text{ primer} \\ \wedge \\ p>q>3 \end{matrix}\right\} \Rightarrow \begin{cases} p \neq \dot{3} \\ \wedge \\ p \text{ senar} \end{cases} \Rightarrow \cdots \Rightarrow 24 \mid (p^2-1) \quad (b)$$

Així doncs, en relació a $p^2-q^2\,(>0)$ es pot concloure que:

$$\left.\begin{matrix} (a) \\ \wedge \\ (b) \end{matrix}\right\} \Rightarrow 24 \mid ((p^2-1)-(q^2-1)) \Rightarrow 24 \mid (p^2-q^2) \Rightarrow \boxed{p^2-q^2=\dot{24}}$$