En torno del teorema de dos cuadrados

$(n = x^2 + y^2)$

Alexey Beshenov

11/11/2021

Motivación

IWYMIC 2004: ¿Cuántas soluciones enteras tiene la ecuación $x^2 + y^2 - 16y = 2004$?

La vez pasada

Para un primo impar p la congruencia $x^2 \equiv -1 \pmod{p}$ tiene solución si y solo si $p \equiv 1 \pmod{4}$.

Ejercicio: Demuestre que $x^2 + y^2 \equiv 0 \pmod{p}$ tiene una solución $(x, y) \not\equiv (0, 0) \pmod{p}$ si y solo si $p \equiv 1 \pmod{4}$.

- Si $y \not\equiv 0$, entonces existe y^{-1} tal que $yy^{-1} \equiv 1 \pmod{p}$.
- $x^2 + y^2 \equiv 0, y \not\equiv 0 \implies (xy^{-1})^2 \equiv -1 \implies p \equiv 1 \pmod{4}$.
- $p \equiv 1 \pmod{4} \implies \exists z, z^2 \equiv -1$.
  Para cualquier x, tenemos $x^2 + (\pm zx)^2 \equiv 0$.

La vez pasada

Para un primo impar p la congruencia $x^2 \equiv -1 \pmod{p}$ tiene solución si y solo si $p \equiv 1 \pmod{4}$.

Ejercicio: Demuestre que $x^2 + y^2 \equiv 0 \pmod{p}$ tiene una solución $(x, y) \not\equiv (0, 0) \pmod{p}$ si y solo si $p \equiv 1 \pmod{4}$.

- Si $y \not\equiv 0$, entonces existe y^{-1} tal que $yy^{-1} \equiv 1 \pmod{p}$.
- $x^2 + y^2 \equiv 0, y \not\equiv 0 \implies (xy^{-1})^2 \equiv -1 \implies p \equiv 1 \pmod{4}$.
- $p \equiv 1 \pmod{4} \implies \exists z, z^2 \equiv -1$.
  Para cualquier x, tenemos $x^2 + (\pm zx)^2 \equiv 0$.

La vez pasada

Para un primo impar p la congruencia $x^2 \equiv -1 \pmod{p}$ tiene solución si y solo si $p \equiv 1 \pmod{4}$.

Ejercicio: Demuestre que $x^2 + y^2 \equiv 0 \pmod{p}$ tiene una solución $(x, y) \not\equiv (0, 0) \pmod{p}$ si y solo si $p \equiv 1 \pmod{4}$.

- Si $y \not\equiv 0$, entonces existe y^{-1} tal que $yy^{-1} \equiv 1 \pmod{p}$.
- $x^2 + y^2 \equiv 0, y \not\equiv 0 \implies (xy^{-1})^2 \equiv -1 \implies p \equiv 1 \pmod{4}$.
- $p \equiv 1 \pmod{4} \implies \exists z, z^2 \equiv -1$.
  Para cualquier x, tenemos $x^2 + (\pm zx)^2 \equiv 0$.

La vez pasada

Para un primo impar p la congruencia $x^2 \equiv -1 \pmod{p}$ tiene solución si y solo si $p \equiv 1 \pmod{4}$.

Ejercicio: Demuestre que $x^2 + y^2 \equiv 0 \pmod{p}$ tiene una solución $(x, y) \not\equiv (0, 0) \pmod{p}$ si y solo si $p \equiv 1 \pmod{4}$.

- Si $y \not\equiv 0$, entonces existe y^{-1} tal que $yy^{-1} \equiv 1 \pmod{p}$.
- $x^2 + y^2 \equiv 0, y \not\equiv 0 \implies (xy^{-1})^2 \equiv -1 \implies p \equiv 1 \pmod{4}$.
- $p \equiv 1 \pmod{4} \implies \exists z, z^2 \equiv -1$.
  Para cualquier x, tenemos $x^2 + (\pm zx)^2 \equiv 0$.

La vez pasada

Para un primo impar p la congruencia $x^2 \equiv -1 \pmod{p}$ tiene solución si y solo si $p \equiv 1 \pmod{4}$.

Ejercicio: Demuestre que $x^2 + y^2 \equiv 0 \pmod{p}$ tiene una solución $(x, y) \not\equiv (0, 0) \pmod{p}$ si y solo si $p \equiv 1 \pmod{4}$.

- Si $y \not\equiv 0$, entonces existe y^{-1} tal que $yy^{-1} \equiv 1 \pmod{p}$.
- $x^2 + y^2 \equiv 0, y \not\equiv 0 \implies (xy^{-1})^2 \equiv -1 \implies p \equiv 1 \pmod{4}$.
- $p \equiv 1 \pmod{4} \implies \exists z, z^2 \equiv -1$.
  Para cualquier x, tenemos $x^2 + (\pm zx)^2 \equiv 0$.

La vez pasada

Para un primo impar p la congruencia $x^2 \equiv -1 \pmod{p}$ tiene solución si y solo si $p \equiv 1 \pmod{4}$.

Ejercicio: Demuestre que $x^2 + y^2 \equiv 0 \pmod{p}$ tiene una solución $(x, y) \not\equiv (0, 0) \pmod{p}$ si y solo si $p \equiv 1 \pmod{4}$.

- Si $y \not\equiv 0$, entonces existe y^{-1} tal que $yy^{-1} \equiv 1 \pmod{p}$.
- $x^2 + y^2 \equiv 0, y \not\equiv 0 \implies (xy^{-1})^2 \equiv -1 \implies p \equiv 1 \pmod{4}$.
- $p \equiv 1 \pmod{4} \implies \exists z, z^2 \equiv -1$.
  Para cualquier x, tenemos $x^2 + (\pm zx)^2 \equiv 0$.

Ejemplo numérico

$$x^2 + y^2 \equiv 0 \pmod{p}$$

- $p = 5$.
- $(\pm 2)^2 \equiv 4 \equiv -1$.
- Ejemplo: $x = 2$, $y = \pm 2x = \pm 4$.
- $(x, y) =$
  $(0, 0), (1, 2), (1, 3), (2, 1), (2, 4), (3, 1), (3, 4), (4, 2), (4, 3)$.

Ejemplo numérico

$$x^2 + y^2 \equiv 0 \pmod{p}$$

- $p = 5$.
- $(\pm 2)^2 \equiv 4 \equiv -1$.
- Ejemplo: $x = 2$, $y = \pm 2x = \pm 4$.
- $(x, y) =$
  $(0,0), (1,2), (1,3), (2,1), (2,4), (3,1), (3,4), (4,2), (4,3)$.

Ejemplo numérico

$$x^2 + y^2 \equiv 0 \pmod{p}$$

- $p = 5$.
- $(\pm 2)^2 \equiv 4 \equiv -1$.
- Ejemplo: $x = 2$, $y = \pm 2x = \pm 4$.
- $(x, y) =$
  $(0,0), (1,2), (1,3), (2,1), (2,4), (3,1), (3,4), (4,2), (4,3)$.

Ejemplo numérico

$$x^2 + y^2 \equiv 0 \pmod{p}$$

- $p = 5$.
- $(\pm 2)^2 \equiv 4 \equiv -1$.
- Ejemplo: $x = 2$, $y = \pm 2x = \pm 4$.
- $(x, y) =$
  $(0,0), (1,2), (1,3), (2,1), (2,4), (3,1), (3,4), (4,2), (4,3)$.

Ejemplo numérico

$$x^2 + y^2 \equiv 0 \pmod{p}$$

- $p = 5$.
- $(\pm 2)^2 \equiv 4 \equiv -1$.
- Ejemplo: $x = 2$, $y = \pm 2x = \pm 4$.
- $(x, y) =$
  $(0, 0)$, $(1, 2)$, $(1, 3)$, $(2, 1)$, $(2, 4)$, $(3, 1)$, $(3, 4)$, $(4, 2)$, $(4, 3)$.

IWYMIC 2004

¿Cuántas soluciones enteras tiene la ecuación
$x^2 + y^2 - 16y = 2004$?

- $x^2 + (y-8)^2 = 2068 = 4 \cdot 11 \cdot 47$.
  Pongamos $z = y - 8$.
- $11 \equiv 47 \equiv 3 \pmod 4$.
- $x^2 + z^2 \equiv 0 \pmod{11}$.
  $x \equiv z \equiv 0 \pmod{11}$ (¡no hay soluciones no triviales!)
- $11 \mid x, 11 \mid z \Longrightarrow 11^2 \mid (x^2 + z^2)$.
  Contradicción.
- Conclusión: ¡no hay soluciones!

IWYMIC 2004

¿Cuántas soluciones enteras tiene la ecuación
$x^2 + y^2 - 16y = 2004$?

- $x^2 + (y-8)^2 = 2068 = 4 \cdot 11 \cdot 47$.
  Pongamos $z = y - 8$.
- $11 \equiv 47 \equiv 3 \pmod 4$.
- $x^2 + z^2 \equiv 0 \pmod{11}$.
  $x \equiv z \equiv 0 \pmod{11}$ (¡no hay soluciones no triviales!)
- $11 \mid x, 11 \mid z \Longrightarrow 11^2 \mid (x^2 + z^2)$.
  Contradicción.
- Conclusión: ¡no hay soluciones!

IWYMIC 2004

¿Cuántas soluciones enteras tiene la ecuación
$x^2 + y^2 - 16y = 2004$?

- $x^2 + (y-8)^2 = 2068 = 4 \cdot 11 \cdot 47$.
  Pongamos $z = y - 8$.
- $11 \equiv 47 \equiv 3 \pmod 4$.
- $x^2 + z^2 \equiv 0 \pmod{11}$.
  $x \equiv z \equiv 0 \pmod{11}$ (¡no hay soluciones no triviales!)
- $11 \mid x, 11 \mid z \Longrightarrow 11^2 \mid (x^2 + z^2)$.
  Contradicción.
- Conclusión: ¡no hay soluciones!

IWYMIC 2004

¿Cuántas soluciones enteras tiene la ecuación $x^2 + y^2 - 16y = 2004$?

- $x^2 + (y-8)^2 = 2068 = 4 \cdot 11 \cdot 47$.
  Pongamos $z = y - 8$.
- $11 \equiv 47 \equiv 3 \pmod 4$.
- $x^2 + z^2 \equiv 0 \pmod{11}$.
  $x \equiv z \equiv 0 \pmod{11}$ (¡no hay soluciones no triviales!)
- $11 \mid x, 11 \mid z \Longrightarrow 11^2 \mid (x^2 + z^2)$.
  Contradicción.
- Conclusión: ¡no hay soluciones!

IWYMIC 2004

¿Cuántas soluciones enteras tiene la ecuación
$x^2 + y^2 - 16y = 2004$?

- $x^2 + (y-8)^2 = 2068 = 4 \cdot 11 \cdot 47$.
  Pongamos $z = y - 8$.
- $11 \equiv 47 \equiv 3 \pmod 4$.
- $x^2 + z^2 \equiv 0 \pmod{11}$.
  $x \equiv z \equiv 0 \pmod{11}$ (¡no hay soluciones no triviales!)
- $11 \mid x, 11 \mid z \Longrightarrow 11^2 \mid (x^2 + z^2)$.
  Contradicción.
- Conclusión: ¡no hay soluciones!

IWYMIC 2004

¿Cuántas soluciones enteras tiene la ecuación
$x^2 + y^2 - 16y = 2004$?

- $x^2 + (y-8)^2 = 2068 = 4 \cdot 11 \cdot 47$.
  Pongamos $z = y - 8$.
- $11 \equiv 47 \equiv 3 \pmod 4$.
- $x^2 + z^2 \equiv 0 \pmod{11}$.
  $x \equiv z \equiv 0 \pmod{11}$ (¡no hay soluciones no triviales!)
- $11 \mid x, 11 \mid z \Longrightarrow 11^2 \mid (x^2 + z^2)$.
  Contradicción.
- Conclusión: ¡no hay soluciones!

IWYMIC 2004

¿Cuántas soluciones enteras tiene la ecuación
$x^2 + y^2 - 16y = 2004$?

- $x^2 + (y-8)^2 = 2068 = 4 \cdot 11 \cdot 47$.
  Pongamos $z = y - 8$.
- $11 \equiv 47 \equiv 3 \pmod 4$.
- $x^2 + z^2 \equiv 0 \pmod{11}$.
  $x \equiv z \equiv 0 \pmod{11}$ (¡no hay soluciones no triviales!)
- $11 \mid x, 11 \mid z \Longrightarrow 11^2 \mid (x^2 + z^2)$.
  Contradicción.
- Conclusión: ¡no hay soluciones!

Pequeña variación

Tarea: Verifique si $x^2 + y^2 - 16y = 2020$ tiene soluciones.

- $x^2 + (y-8)^2 = 2084 = 2^2 \cdot 521$.
- $521 \equiv 1 \pmod 4$ y $521 = 11^2 + 20^2$.
- **Identidad de Diofanto** (ejercicio):
  $(a^2 + b^2)(c^2 + d^2) = (ac - bd)^2 + (ad + bc)^2$.
- $2084 = 2^2 \cdot 521 = (0 + 2^2)(11^2 + 20^2) = 22^2 + 40^2$.
- $x = 22, y = 48$ es una solución.
- 8 soluciones en total, que vinenen de
  $2084 = (\pm 22)^2 + (\pm 40)^2 = (\pm 40)^2 + (\pm 22)^2$.

Pequeña variación

Tarea: Verifique si $x^2 + y^2 - 16y = 2020$ tiene soluciones.

- $x^2 + (y-8)^2 = 2084 = 2^2 \cdot 521$.
- $521 \equiv 1 \pmod 4$ y $521 = 11^2 + 20^2$.
- **Identidad de Diofanto** (ejercicio):
  $(a^2 + b^2)(c^2 + d^2) = (ac - bd)^2 + (ad + bc)^2$.
- $2084 = 2^2 \cdot 521 = (0 + 2^2)(11^2 + 20^2) = 22^2 + 40^2$.
- $x = 22, y = 48$ es una solución.
- 8 soluciones en total, que vinenen de
  $2084 = (\pm 22)^2 + (\pm 40)^2 = (\pm 40)^2 + (\pm 22)^2$.

Pequeña variación

Tarea: Verifique si $x^2 + y^2 - 16y = 2020$ tiene soluciones.

- $x^2 + (y-8)^2 = 2084 = 2^2 \cdot 521$.
- $521 \equiv 1 \pmod 4$ y $521 = 11^2 + 20^2$.
- **Identidad de Diofanto** (ejercicio):
  $(a^2 + b^2)(c^2 + d^2) = (ac - bd)^2 + (ad + bc)^2$.
- $2084 = 2^2 \cdot 521 = (0 + 2^2)(11^2 + 20^2) = 22^2 + 40^2$.
- $x = 22, y = 48$ es una solución.
- 8 soluciones en total, que vinenen de
  $2084 = (\pm 22)^2 + (\pm 40)^2 = (\pm 40)^2 + (\pm 22)^2$.

Pequeña variación

Tarea: Verifique si $x^2 + y^2 - 16y = 2020$ tiene soluciones.

- $x^2 + (y-8)^2 = 2084 = 2^2 \cdot 521$.
- $521 \equiv 1 \pmod 4$ y $521 = 11^2 + 20^2$.
- **Identidad de Diofanto** (ejercicio):
  $(a^2 + b^2)(c^2 + d^2) = (ac - bd)^2 + (ad + bc)^2$.
- $2084 = 2^2 \cdot 521 = (0 + 2^2)(11^2 + 20^2) = 22^2 + 40^2$.
- $x = 22, y = 48$ es una solución.
- 8 soluciones en total, que vinenen de
  $2084 = (\pm 22)^2 + (\pm 40)^2 = (\pm 40)^2 + (\pm 22)^2$.

Pequeña variación

Tarea: Verifique si $x^2 + y^2 - 16y = 2020$ tiene soluciones.

- $x^2 + (y-8)^2 = 2084 = 2^2 \cdot 521$.
- $521 \equiv 1 \pmod 4$ y $521 = 11^2 + 20^2$.
- **Identidad de Diofanto** (ejercicio):
  $(a^2 + b^2)(c^2 + d^2) = (ac - bd)^2 + (ad + bc)^2$.
- $2084 = 2^2 \cdot 521 = (0 + 2^2)(11^2 + 20^2) = 22^2 + 40^2$.
- $x = 22, y = 48$ es una solución.
- 8 soluciones en total, que vinenen de
  $2084 = (\pm 22)^2 + (\pm 40)^2 = (\pm 40)^2 + (\pm 22)^2$.

Pequeña variación

Tarea: Verifique si $x^2 + y^2 - 16y = 2020$ tiene soluciones.

- $x^2 + (y-8)^2 = 2084 = 2^2 \cdot 521$.
- $521 \equiv 1 \pmod 4$ y $521 = 11^2 + 20^2$.
- **Identidad de Diofanto** (ejercicio):
  $(a^2 + b^2)(c^2 + d^2) = (ac - bd)^2 + (ad + bc)^2$.
- $2084 = 2^2 \cdot 521 = (0 + 2^2)(11^2 + 20^2) = 22^2 + 40^2$.
- $x = 22, y = 48$ es una solución.
- 8 soluciones en total, que vinenen de
  $2084 = (\pm 22)^2 + (\pm 40)^2 = (\pm 40)^2 + (\pm 22)^2$.

Pequeña variación

Tarea: Verifique si $x^2 + y^2 - 16y = 2020$ tiene soluciones.

- $x^2 + (y-8)^2 = 2084 = 2^2 \cdot 521$.
- $521 \equiv 1 \pmod 4$ y $521 = 11^2 + 20^2$.
- **Identidad de Diofanto** (ejercicio):
  $(a^2 + b^2)(c^2 + d^2) = (ac - bd)^2 + (ad + bc)^2$.
- $2084 = 2^2 \cdot 521 = (0 + 2^2)(11^2 + 20^2) = 22^2 + 40^2$.
- $x = 22, y = 48$ es una solución.
- 8 soluciones en total, que vinenen de
  $2084 = (\pm 22)^2 + (\pm 40)^2 = (\pm 40)^2 + (\pm 22)^2$.

Pequeña variación

Tarea: Verifique si $x^2 + y^2 - 16y = 2020$ tiene soluciones.

- $x^2 + (y-8)^2 = 2084 = 2^2 \cdot 521$.
- $521 \equiv 1 \pmod 4$ y $521 = 11^2 + 20^2$.
- **Identidad de Diofanto** (ejercicio):
  $(a^2 + b^2)(c^2 + d^2) = (ac - bd)^2 + (ad + bc)^2$.
- $2084 = 2^2 \cdot 521 = (0 + 2^2)(11^2 + 20^2) = 22^2 + 40^2$.
- $x = 22, y = 48$ es una solución.
- 8 soluciones en total, que vinenen de
  $2084 = (\pm 22)^2 + (\pm 40)^2 = (\pm 40)^2 + (\pm 22)^2$.

Teorema de dos cuadrados

Fermat (1640): Un primo impar p es una suma de dos cuadrados si y solamente si $p \equiv 1 \pmod 4$.
Primera prueba: Euler (1749).

$$5 = 1^2 + 2^2, \quad 13 = 2^2 + 3^2, \quad 17 = 1^2 + 4^2,$$
$$29 = 2^2 + 5^2, \quad 37 = 1^2 + 6^2, \quad 41 = 4^2 + 5^2,$$
$$53 = 2^2 + 7^2, \quad 61 = 5^2 + 6^2, \quad 73 = 3^2 + 8^2,$$
$$89 = 5^2 + 8^2, \quad 97 = 4^2 + 9^2, \quad 101 = 1^2 + 10^2,$$
$$109 = 3^2 + 10^2, \quad 113 = 7^2 + 8^2, \quad 137 = 4^2 + 11^2,$$
$$149 = 7^2 + 10^2, \quad 157 = 6^2 + 11^2, \quad 173 = 2^2 + 13^2.$$

Teorema de dos cuadrados

Fermat (1640): Un primo impar p es una suma de dos cuadrados si y solamente si $p \equiv 1 \pmod 4$.
Primera prueba: Euler (1749).

$$
\begin{aligned}
5 &= 1^2 + 2^2, & 13 &= 2^2 + 3^2, & 17 &= 1^2 + 4^2,\\
29 &= 2^2 + 5^2, & 37 &= 1^2 + 6^2, & 41 &= 4^2 + 5^2,\\
53 &= 2^2 + 7^2, & 61 &= 5^2 + 6^2, & 73 &= 3^2 + 8^2,\\
89 &= 5^2 + 8^2, & 97 &= 4^2 + 9^2, & 101 &= 1^2 + 10^2,\\
109 &= 3^2 + 10^2, & 113 &= 7^2 + 8^2, & 137 &= 4^2 + 11^2,\\
149 &= 7^2 + 10^2, & 157 &= 6^2 + 11^2, & 173 &= 2^2 + 13^2.
\end{aligned}
$$

Prueba (Thue, 1902)

Necesidad (fácil):

- $p = x^2 + y^2 \Longrightarrow x^2 + y^2 \equiv 0 \pmod{p}, (x, y) \not\equiv (0, 0)$
  $\Longrightarrow p \equiv 1 \pmod{4}$.

Suficiencia (difícil):

- $p \equiv 1 \pmod{4} \Longrightarrow z^2 \equiv -1$ tiene solución.
- $S = \{(x', y') \in \mathbb{Z}^2 \mid 0 \leq x', y' \leq \sqrt{p}\}$.
- $|S| = (\lfloor \sqrt{p} \rfloor + 1)^2 > p$.
  Principio de las casillas: $(x', y') \neq (x'', y'')$ tales que

$$x' - zy' \equiv x'' - zy'' \pmod{p} \iff x' - x'' \equiv z\,(y' - y'').$$

- $x = |x' - x''|, y = |y' - y''|$.
- $x^2 + y^2 \equiv 0 \pmod{p}, 0 < x^2 + y^2 < 2p$,
  $\Longrightarrow x^2 + y^2 = p$. □

Prueba (Thue, 1902)

Necesidad (fácil):

- $p = x^2 + y^2 \Longrightarrow x^2 + y^2 \equiv 0 \pmod{p}, (x, y) \not\equiv (0, 0)$
  $\Longrightarrow p \equiv 1 \pmod{4}$.

Suficiencia (difícil):

- $p \equiv 1 \pmod{4} \Longrightarrow z^2 \equiv -1$ tiene solución.
- $S = \{(x', y') \in \mathbb{Z}^2 \mid 0 \leq x', y' \leq \sqrt{p}\}$.
- $|S| = (\lfloor \sqrt{p} \rfloor + 1)^2 > p$.
  Principio de las casillas: $(x', y') \neq (x'', y'')$ tales que

$$x' - zy' \equiv x'' - zy'' \pmod{p} \iff x' - x'' \equiv z\,(y' - y'').$$

- $x = |x' - x''|, y = |y' - y''|$.
- $x^2 + y^2 \equiv 0 \pmod{p}, 0 < x^2 + y^2 < 2p$,
  $\Longrightarrow x^2 + y^2 = p$. □

Prueba (Thue, 1902)

Necesidad (fácil):

- $p = x^2 + y^2 \Longrightarrow x^2 + y^2 \equiv 0 \pmod{p}, (x, y) \not\equiv (0, 0)$
  $\Longrightarrow p \equiv 1 \pmod{4}$.

Suficiencia (difícil):

- $p \equiv 1 \pmod{4} \Longrightarrow z^2 \equiv -1$ tiene solución.
- $S = \{(x', y') \in \mathbb{Z}^2 \mid 0 \leq x', y' \leq \sqrt{p}\}$.
- $|S| = (\lfloor \sqrt{p} \rfloor + 1)^2 > p$.
  Principio de las casillas: $(x', y') \neq (x'', y'')$ tales que

$$x' - zy' \equiv x'' - zy'' \pmod{p} \iff x' - x'' \equiv z\,(y' - y'').$$

- $x = |x' - x''|, y = |y' - y''|$.
- $x^2 + y^2 \equiv 0 \pmod{p}, 0 < x^2 + y^2 < 2p$,
  $\Longrightarrow x^2 + y^2 = p$. □

Prueba (Thue, 1902)

Necesidad (fácil):

- $p = x^2 + y^2 \Longrightarrow x^2 + y^2 \equiv 0 \pmod{p}, (x, y) \not\equiv (0, 0)$
  $\Longrightarrow p \equiv 1 \pmod{4}$.

Suficiencia (difícil):

- $p \equiv 1 \pmod{4} \Longrightarrow z^2 \equiv -1$ tiene solución.
- $S = \{(x', y') \in \mathbb{Z}^2 \mid 0 \leq x', y' \leq \sqrt{p}\}$.
- $|S| = (\lfloor \sqrt{p} \rfloor + 1)^2 > p$.
  Principio de las casillas: $(x', y') \neq (x'', y'')$ tales que

$$x' - zy' \equiv x'' - zy'' \pmod{p} \iff x' - x'' \equiv z\,(y' - y'').$$

- $x = |x' - x''|, y = |y' - y''|$.
- $x^2 + y^2 \equiv 0 \pmod{p}, 0 < x^2 + y^2 < 2p$,
  $\Longrightarrow x^2 + y^2 = p$. □

Prueba (Thue, 1902)

Necesidad (fácil):

- $p = x^2 + y^2 \Longrightarrow x^2 + y^2 \equiv 0 \pmod{p}, (x, y) \not\equiv (0, 0)$
  $\Longrightarrow p \equiv 1 \pmod{4}$.

Suficiencia (difícil):

- $p \equiv 1 \pmod{4} \Longrightarrow z^2 \equiv -1$ tiene solución.
- $S = \{(x', y') \in \mathbb{Z}^2 \mid 0 \leq x', y' \leq \sqrt{p}\}$.
- $|S| = (\lfloor \sqrt{p} \rfloor + 1)^2 > p$.
  Principio de las casillas: $(x', y') \neq (x'', y'')$ tales que

$$x' - zy' \equiv x'' - zy'' \pmod{p} \iff x' - x'' \equiv z\,(y' - y'').$$

- $x = |x' - x''|, y = |y' - y''|$.
- $x^2 + y^2 \equiv 0 \pmod{p}, 0 < x^2 + y^2 < 2p$,
  $\Longrightarrow x^2 + y^2 = p$. □

Prueba (Thue, 1902)

Necesidad (fácil):

- $p = x^2 + y^2 \Longrightarrow x^2 + y^2 \equiv 0 \pmod{p}, (x, y) \not\equiv (0, 0)$
  $\Longrightarrow p \equiv 1 \pmod{4}$.

Suficiencia (difícil):

- $p \equiv 1 \pmod{4} \Longrightarrow z^2 \equiv -1$ tiene solución.
- $S = \{(x', y') \in \mathbb{Z}^2 \mid 0 \leq x', y' \leq \sqrt{p}\}$.
- $|S| = (\lfloor \sqrt{p} \rfloor + 1)^2 > p$.
  Principio de las casillas: $(x', y') \neq (x'', y'')$ tales que

$$x' - zy' \equiv x'' - zy'' \pmod{p} \iff x' - x'' \equiv z\,(y' - y'').$$

- $x = |x' - x''|, y = |y' - y''|$.
- $x^2 + y^2 \equiv 0 \pmod{p}, 0 < x^2 + y^2 < 2p$,
  $\Longrightarrow x^2 + y^2 = p$. □

Prueba (Thue, 1902)

Necesidad (fácil):

- $p = x^2 + y^2 \Longrightarrow x^2 + y^2 \equiv 0 \pmod{p}, (x, y) \not\equiv (0, 0)$
  $\Longrightarrow p \equiv 1 \pmod{4}$.

Suficiencia (difícil):

- $p \equiv 1 \pmod{4} \Longrightarrow z^2 \equiv -1$ tiene solución.
- $S = \{(x', y') \in \mathbb{Z}^2 \mid 0 \leq x', y' \leq \sqrt{p}\}$.
- $|S| = (\lfloor \sqrt{p} \rfloor + 1)^2 > p$.
  Principio de las casillas: $(x', y') \neq (x'', y'')$ tales que

$$x' - zy' \equiv x'' - zy'' \pmod{p} \iff x' - x'' \equiv z\,(y' - y'').$$

- $x = |x' - x''|, y = |y' - y''|$.
- $x^2 + y^2 \equiv 0 \pmod{p}, 0 < x^2 + y^2 < 2p$,
  $\Longrightarrow x^2 + y^2 = p$. □

Prueba (Thue, 1902)

Necesidad (fácil):

- $p = x^2 + y^2 \Longrightarrow x^2 + y^2 \equiv 0 \pmod{p}, (x, y) \not\equiv (0, 0)$
  $\Longrightarrow p \equiv 1 \pmod{4}$.

Suficiencia (difícil):

- $p \equiv 1 \pmod{4} \Longrightarrow z^2 \equiv -1$ tiene solución.
- $S = \{(x', y') \in \mathbb{Z}^2 \mid 0 \leq x', y' \leq \sqrt{p}\}$.
- $|S| = (\lfloor \sqrt{p} \rfloor + 1)^2 > p$.
  Principio de las casillas: $(x', y') \neq (x'', y'')$ tales que

$$x' - zy' \equiv x'' - zy'' \pmod{p} \iff x' - x'' \equiv z\,(y' - y'').$$

- $x = |x' - x''|, y = |y' - y''|$.
- $x^2 + y^2 \equiv 0 \pmod{p}, 0 < x^2 + y^2 < 2p,$
  $\Longrightarrow x^2 + y^2 = p$. □

Prueba (Thue, 1902)

Necesidad (fácil):

- $p = x^2 + y^2 \Longrightarrow x^2 + y^2 \equiv 0 \pmod{p}, (x, y) \not\equiv (0, 0)$
  $\Longrightarrow p \equiv 1 \pmod{4}$.

Suficiencia (difícil):

- $p \equiv 1 \pmod{4} \Longrightarrow z^2 \equiv -1$ tiene solución.
- $S = \{(x', y') \in \mathbb{Z}^2 \mid 0 \leq x', y' \leq \sqrt{p}\}$.
- $|S| = (\lfloor \sqrt{p} \rfloor + 1)^2 > p$.
  Principio de las casillas: $(x', y') \neq (x'', y'')$ tales que

$$x' - zy' \equiv x'' - zy'' \pmod{p} \iff x' - x'' \equiv z\,(y' - y'').$$

- $x = |x' - x''|, y = |y' - y''|$.
- $x^2 + y^2 \equiv 0 \pmod{p}, 0 < x^2 + y^2 < 2p$,
  $\Longrightarrow x^2 + y^2 = p$. □

Ejemplo numérico

- $p = 29$, $\lfloor \sqrt{p} \rfloor = 5$.
- $12^2 \equiv -1 \pmod{p}$.
- Consideremos $x' - 12\,y' \pmod{p}$, $0 < x', y' \leq 5$.

x' \ y'	0	1	2	3	4	5
0	0	17	5	22	10	27
1	1	18	6	23	11	28
2	2	19	7	24	12	0
3	3	20	8	25	13	1
4	4	21	9	26	14	2
5	5	22	10	27	15	3

- $1 - 12 \cdot 0 \equiv 3 - 12 \cdot 5 \iff 1 - 3 \equiv 12 \cdot (0 - 5)$.
- $(1 - 3)^2 + (0 - 5)^2 \equiv 0$.
- $29 = 2^2 + 5^2$.

Ejemplo numérico

- $p = 29$, $\lfloor \sqrt{p} \rfloor = 5$.
- $12^2 \equiv -1 \pmod{p}$.
- Consideremos $x' - 12\,y' \pmod{p}$, $0 < x', y' \leq 5$.

x' \ y'	0	1	2	3	4	5
0	0	17	5	22	10	27
1	**1**	18	6	23	11	28
2	2	19	7	24	12	0
3	3	20	8	25	13	**1**
4	4	21	9	26	14	2
5	5	22	10	27	15	3

- $1 - 12 \cdot 0 \equiv 3 - 12 \cdot 5 \iff 1 - 3 \equiv 12 \cdot (0 - 5)$.
- $(1-3)^2 + (0-5)^2 \equiv 0$.
- $29 = 2^2 + 5^2$.

Ejemplo numérico

- $p = 29$, $\lfloor \sqrt{p} \rfloor = 5$.
- $12^2 \equiv -1 \pmod{p}$.
- Consideremos $x' - 12\,y' \pmod{p}$, $0 < x', y' \leq 5$.

x' \ y'	0	1	2	3	4	5
0	0	17	5	22	10	27
1	**1**	18	6	23	11	28
2	2	19	7	24	12	0
3	3	20	8	25	13	**1**
4	4	21	9	26	14	2
5	5	22	10	27	15	3

- $1 - 12 \cdot 0 \equiv 3 - 12 \cdot 5 \iff 1 - 3 \equiv 12 \cdot (0 - 5)$.
- $(1-3)^2 + (0-5)^2 \equiv 0$.
- $29 = 2^2 + 5^2$.

Ejemplo numérico

- $p = 29$, $\lfloor \sqrt{p} \rfloor = 5$.
- $12^2 \equiv -1 \pmod{p}$.
- Consideremos $x' - 12\,y' \pmod{p}$, $0 < x', y' \leq 5$.

x' \ y'	0	1	2	3	4	5
0	0	17	5	22	10	27
1	1	18	6	23	11	28
2	2	19	7	24	12	0
3	3	20	8	25	13	1
4	4	21	9	26	14	2
5	5	22	10	27	15	3

- $1 - 12 \cdot 0 \equiv 3 - 12 \cdot 5 \iff 1 - 3 \equiv 12 \cdot (0 - 5)$.
- $(1 - 3)^2 + (0 - 5)^2 \equiv 0$.
- $29 = 2^2 + 5^2$.

Ejemplo numérico

- $p = 29$, $\lfloor \sqrt{p} \rfloor = 5$.
- $12^2 \equiv -1 \pmod{p}$.
- Consideremos $x' - 12\,y' \pmod{p}$, $0 < x', y' \leq 5$.

x' \ y'	0	1	2	3	4	5
0	0	17	5	22	10	27
1	**1**	18	6	23	11	28
2	2	19	7	24	12	0
3	3	20	8	25	13	**1**
4	4	21	9	26	14	2
5	5	22	10	27	15	3

- $1 - 12 \cdot 0 \equiv 3 - 12 \cdot 5 \iff 1 - 3 \equiv 12 \cdot (0 - 5)$.
- $(1 - 3)^2 + (0 - 5)^2 \equiv 0$.
- $29 = 2^2 + 5^2$.

Ejemplo numérico

- $p = 29$, $\lfloor \sqrt{p} \rfloor = 5$.
- $12^2 \equiv -1 \pmod{p}$.
- Consideremos $x' - 12\,y' \pmod{p}$, $0 < x', y' \leq 5$.

x' \ y'	0	1	2	3	4	5
0	0	17	5	22	10	27
1	**1**	18	6	23	11	28
2	2	19	7	24	12	0
3	3	20	8	25	13	**1**
4	4	21	9	26	14	2
5	5	22	10	27	15	3

- $1 - 12 \cdot 0 \equiv 3 - 12 \cdot 5 \iff 1 - 3 \equiv 12 \cdot (0 - 5)$.
- $(1 - 3)^2 + (0 - 5)^2 \equiv 0$.
- $29 = 2^2 + 5^2$.

Ejemplo numérico

- $p = 29$, $\lfloor \sqrt{p} \rfloor = 5$.
- $12^2 \equiv -1 \pmod{p}$.
- Consideremos $x' - 12\,y' \pmod{p}$, $0 < x', y' \leq 5$.

x' \ y'	0	1	2	3	4	5
0	0	17	5	22	10	27
1	$\boxed{1}$	18	6	23	11	28
2	2	19	7	24	12	0
3	3	20	8	25	13	$\boxed{1}$
4	4	21	9	26	14	2
5	5	22	10	27	15	3

- $1 - 12 \cdot 0 \equiv 3 - 12 \cdot 5 \iff 1 - 3 \equiv 12 \cdot (0 - 5)$.
- $(1 - 3)^2 + (0 - 5)^2 \equiv 0$.
- $29 = 2^2 + 5^2$.

Números compuestos

$n = p_1^{e_1} \cdots p_s^{e_s}$ es una suma de dos cuadrados si y solo si cada $p_i \equiv 3 \pmod 4$ tiene potencia par e_i.

Suficiencia:

- $1 = 1^2 + 0^2, 2 = 1^2 + 1^2$.
- Si $p \equiv 1 \pmod 4$, entonces $p = x^2 + y^2$.
- Si $m = a^2 + b^2, n = c^2 + d^2$, $mn = (ac - bd)^2 + (ad + bc)^2$.
- Si $m = a^2 + b^2$, entonces $mn^2 = (an)^2 + (bn)^2$.

Necesidad:

- $n = x^2 + y^2, p_i \mid n, p_i \equiv 3 \pmod 4$.
- $p_i \mid x, p_i \mid y \Longrightarrow p_i^2 \mid n, n/p_i^2 = (x/p_i)^2 + (y/p_i)^2$.
- $n/p_i^2 = p_1^{e_1} \cdots p_i^{e_i - 2} \cdots p_s^{e_s}$.
- Si $p_i \equiv 3 \pmod 4$, entonces $p_i \neq \square + \square$.

Números compuestos

$n = p_1^{e_1} \cdots p_s^{e_s}$ es una suma de dos cuadrados si y solo si cada $p_i \equiv 3 \pmod 4$ tiene potencia par e_i.

Suficiencia:

- $1 = 1^2 + 0^2, 2 = 1^2 + 1^2$.
- Si $p \equiv 1 \pmod 4$, entonces $p = x^2 + y^2$.
- Si $m = a^2 + b^2, n = c^2 + d^2$, $mn = (ac - bd)^2 + (ad + bc)^2$.
- Si $m = a^2 + b^2$, entonces $mn^2 = (an)^2 + (bn)^2$.

Necesidad:

- $n = x^2 + y^2, p_i \mid n, p_i \equiv 3 \pmod 4$.
- $p_i \mid x, p_i \mid y \Longrightarrow p_i^2 \mid n, n/p_i^2 = (x/p_i)^2 + (y/p_i)^2$.
- $n/p_i^2 = p_1^{e_1} \cdots p_i^{e_i - 2} \cdots p_s^{e_s}$.
- Si $p_i \equiv 3 \pmod 4$, entonces $p_i \neq \square + \square$.

Números compuestos

$n = p_1^{e_1} \cdots p_s^{e_s}$ es una suma de dos cuadrados si y solo si cada $p_i \equiv 3 \pmod 4$ tiene potencia par e_i.

Suficiencia:

- $1 = 1^2 + 0^2, 2 = 1^2 + 1^2$.
- Si $p \equiv 1 \pmod 4$, entonces $p = x^2 + y^2$.
- Si $m = a^2 + b^2, n = c^2 + d^2$, $mn = (ac - bd)^2 + (ad + bc)^2$.
- Si $m = a^2 + b^2$, entonces $mn^2 = (an)^2 + (bn)^2$.

Necesidad:

- $n = x^2 + y^2, p_i \mid n, p_i \equiv 3 \pmod 4$.
- $p_i \mid x, p_i \mid y \Longrightarrow p_i^2 \mid n, n/p_i^2 = (x/p_i)^2 + (y/p_i)^2$.
- $n/p_i^2 = p_1^{e_1} \cdots p_i^{e_i - 2} \cdots p_s^{e_s}$.
- Si $p_i \equiv 3 \pmod 4$, entonces $p_i \neq \square + \square$.

Números compuestos

$n = p_1^{e_1} \cdots p_s^{e_s}$ es una suma de dos cuadrados si y solo si cada $p_i \equiv 3 \pmod 4$ tiene potencia par e_i.

Suficiencia:

- $1 = 1^2 + 0^2$, $2 = 1^2 + 1^2$.
- Si $p \equiv 1 \pmod 4$, entonces $p = x^2 + y^2$.
- Si $m = a^2 + b^2$, $n = c^2 + d^2$, $mn = (ac - bd)^2 + (ad + bc)^2$.
- Si $m = a^2 + b^2$, entonces $mn^2 = (an)^2 + (bn)^2$.

Necesidad:

- $n = x^2 + y^2$, $p_i \mid n$, $p_i \equiv 3 \pmod 4$.
- $p_i \mid x, p_i \mid y \Longrightarrow p_i^2 \mid n, n/p_i^2 = (x/p_i)^2 + (y/p_i)^2$.
- $n/p_i^2 = p_1^{e_1} \cdots p_i^{e_i - 2} \cdots p_s^{e_s}$.
- Si $p_i \equiv 3 \pmod 4$, entonces $p_i \neq \square + \square$.

Números compuestos

$n = p_1^{e_1} \cdots p_s^{e_s}$ es una suma de dos cuadrados si y solo si cada $p_i \equiv 3 \pmod 4$ tiene potencia par e_i.

Suficiencia:

- $1 = 1^2 + 0^2$, $2 = 1^2 + 1^2$.
- Si $p \equiv 1 \pmod 4$, entonces $p = x^2 + y^2$.
- Si $m = a^2 + b^2$, $n = c^2 + d^2$, $mn = (ac - bd)^2 + (ad + bc)^2$.
- Si $m = a^2 + b^2$, entonces $mn^2 = (an)^2 + (bn)^2$.

Necesidad:

- $n = x^2 + y^2$, $p_i \mid n$, $p_i \equiv 3 \pmod 4$.
- $p_i \mid x, p_i \mid y \Longrightarrow p_i^2 \mid n, n/p_i^2 = (x/p_i)^2 + (y/p_i)^2$.
- $n/p_i^2 = p_1^{e_1} \cdots p_i^{e_i - 2} \cdots p_s^{e_s}$.
- Si $p_i \equiv 3 \pmod 4$, entonces $p_i \neq \square + \square$.

Números compuestos

$n = p_1^{e_1} \cdots p_s^{e_s}$ es una suma de dos cuadrados si y solo si cada $p_i \equiv 3 \pmod 4$ tiene potencia par e_i.

Suficiencia:

- $1 = 1^2 + 0^2$, $2 = 1^2 + 1^2$.
- Si $p \equiv 1 \pmod 4$, entonces $p = x^2 + y^2$.
- Si $m = a^2 + b^2$, $n = c^2 + d^2$, $mn = (ac - bd)^2 + (ad + bc)^2$.
- Si $m = a^2 + b^2$, entonces $mn^2 = (an)^2 + (bn)^2$.

Necesidad:

- $n = x^2 + y^2$, $p_i \mid n$, $p_i \equiv 3 \pmod 4$.
- $p_i \mid x, p_i \mid y \Longrightarrow p_i^2 \mid n, n/p_i^2 = (x/p_i)^2 + (y/p_i)^2$.
- $n/p_i^2 = p_1^{e_1} \cdots p_i^{e_i - 2} \cdots p_s^{e_s}$.
- Si $p_i \equiv 3 \pmod 4$, entonces $p_i \neq \square + \square$.

Números compuestos

$n = p_1^{e_1} \cdots p_s^{e_s}$ es una suma de dos cuadrados si y solo si cada $p_i \equiv 3 \pmod 4$ tiene potencia par e_i.

Suficiencia:

- $1 = 1^2 + 0^2$, $2 = 1^2 + 1^2$.
- Si $p \equiv 1 \pmod 4$, entonces $p = x^2 + y^2$.
- Si $m = a^2 + b^2$, $n = c^2 + d^2$, $mn = (ac - bd)^2 + (ad + bc)^2$.
- Si $m = a^2 + b^2$, entonces $mn^2 = (an)^2 + (bn)^2$.

Necesidad:

- $n = x^2 + y^2$, $p_i \mid n$, $p_i \equiv 3 \pmod 4$.
- $p_i \mid x, p_i \mid y \Longrightarrow p_i^2 \mid n, n/p_i^2 = (x/p_i)^2 + (y/p_i)^2$.
- $n/p_i^2 = p_1^{e_1} \cdots p_i^{e_i - 2} \cdots p_s^{e_s}$.
- Si $p_i \equiv 3 \pmod 4$, entonces $p_i \neq \square + \square$.

Números compuestos

$n = p_1^{e_1} \cdots p_s^{e_s}$ es una suma de dos cuadrados si y solo si cada $p_i \equiv 3 \pmod 4$ tiene potencia par e_i.

Suficiencia:

- $1 = 1^2 + 0^2$, $2 = 1^2 + 1^2$.
- Si $p \equiv 1 \pmod 4$, entonces $p = x^2 + y^2$.
- Si $m = a^2 + b^2$, $n = c^2 + d^2$, $mn = (ac - bd)^2 + (ad + bc)^2$.
- Si $m = a^2 + b^2$, entonces $mn^2 = (an)^2 + (bn)^2$.

Necesidad:

- $n = x^2 + y^2$, $p_i \mid n$, $p_i \equiv 3 \pmod 4$.
- $p_i \mid x, p_i \mid y \Longrightarrow p_i^2 \mid n, n/p_i^2 = (x/p_i)^2 + (y/p_i)^2$.
- $n/p_i^2 = p_1^{e_1} \cdots p_i^{e_i - 2} \cdots p_s^{e_s}$.
- Si $p_i \equiv 3 \pmod 4$, entonces $p_i \neq \square + \square$.

Números compuestos

$n = p_1^{e_1} \cdots p_s^{e_s}$ es una suma de dos cuadrados si y solo si cada $p_i \equiv 3 \pmod 4$ tiene potencia par e_i.

Suficiencia:

- $1 = 1^2 + 0^2$, $2 = 1^2 + 1^2$.
- Si $p \equiv 1 \pmod 4$, entonces $p = x^2 + y^2$.
- Si $m = a^2 + b^2$, $n = c^2 + d^2$,
  $mn = (ac - bd)^2 + (ad + bc)^2$.
- Si $m = a^2 + b^2$, entonces $mn^2 = (an)^2 + (bn)^2$.

Necesidad:

- $n = x^2 + y^2$, $p_i \mid n$, $p_i \equiv 3 \pmod 4$.
- $p_i \mid x, p_i \mid y \Longrightarrow p_i^2 \mid n, n/p_i^2 = (x/p_i)^2 + (y/p_i)^2$.
- $n/p_i^2 = p_1^{e_1} \cdots p_i^{e_i - 2} \cdots p_s^{e_s}$.
- Si $p_i \equiv 3 \pmod 4$, entonces $p_i \neq \square + \square$.

Números compuestos

$n = p_1^{e_1} \cdots p_s^{e_s}$ es una suma de dos cuadrados si y solo si cada $p_i \equiv 3 \pmod 4$ tiene potencia par e_i.

Suficiencia:

- $1 = 1^2 + 0^2$, $2 = 1^2 + 1^2$.
- Si $p \equiv 1 \pmod 4$, entonces $p = x^2 + y^2$.
- Si $m = a^2 + b^2$, $n = c^2 + d^2$, $mn = (ac - bd)^2 + (ad + bc)^2$.
- Si $m = a^2 + b^2$, entonces $mn^2 = (an)^2 + (bn)^2$.

Necesidad:

- $n = x^2 + y^2$, $p_i \mid n$, $p_i \equiv 3 \pmod 4$.
- $p_i \mid x, p_i \mid y \Longrightarrow p_i^2 \mid n, n/p_i^2 = (x/p_i)^2 + (y/p_i)^2$.
- $n/p_i^2 = p_1^{e_1} \cdots p_i^{e_i - 2} \cdots p_s^{e_s}$.
- Si $p_i \equiv 3 \pmod 4$, entonces $p_i \neq \square + \square$.

Números compuestos

$n = p_1^{e_1} \cdots p_s^{e_s}$ es una suma de dos cuadrados si y solo si cada $p_i \equiv 3 \pmod 4$ tiene potencia par e_i.

Suficiencia:

- $1 = 1^2 + 0^2$, $2 = 1^2 + 1^2$.
- Si $p \equiv 1 \pmod 4$, entonces $p = x^2 + y^2$.
- Si $m = a^2 + b^2$, $n = c^2 + d^2$, $mn = (ac - bd)^2 + (ad + bc)^2$.
- Si $m = a^2 + b^2$, entonces $mn^2 = (an)^2 + (bn)^2$.

Necesidad:

- $n = x^2 + y^2$, $p_i \mid n$, $p_i \equiv 3 \pmod 4$.
- $p_i \mid x, p_i \mid y \Longrightarrow p_i^2 \mid n, n/p_i^2 = (x/p_i)^2 + (y/p_i)^2$.
- $n/p_i^2 = p_1^{e_1} \cdots p_i^{e_i - 2} \cdots p_s^{e_s}$.
- Si $p_i \equiv 3 \pmod 4$, entonces $p_i \neq \square + \square$.

Ejercicio

Verifique cuáles de los siguientes números tienen forma $n = x^2 + y^2$. Encuentre x e y correspondiente.

$$n = 160,\ 208,\ 230,\ 351,\ 585,\ 715.$$

$160 = 2^5 \cdot 5$, $160 = 4^2 + 12^2$;

$208 = 2^4 \cdot 13$, $208 = 8^2 + 12^2$;

$230 = 2 \cdot 5 \cdot \boxed{23}$, $230 \neq \square + \square$;

$351 = \boxed{3^3} \cdot 13$, $351 \neq \square + \square$;

$585 = 3^2 \cdot 5 \cdot 13$, $585 = 3^2 + 24^2 = 12^2 + 21^2$;

$715 = 5 \cdot \boxed{11} \cdot 13$, $715 \neq \square + \square$.

Ejercicio

Verifique cuáles de los siguientes números tienen forma $n = x^2 + y^2$. Encuentre x e y correspondiente.

$$n = 160,\ 208,\ 230,\ 351,\ 585,\ 715.$$

$160 = 2^5 \cdot 5$, $160 = 4^2 + 12^2$;

$208 = 2^4 \cdot 13$, $208 = 8^2 + 12^2$;

$230 = 2 \cdot 5 \cdot \boxed{23}$, $230 \neq \square + \square$;

$351 = \boxed{3^3} \cdot 13$, $351 \neq \square + \square$;

$585 = 3^2 \cdot 5 \cdot 13$, $585 = 3^2 + 24^2 = 12^2 + 21^2$;

$715 = 5 \cdot \boxed{11} \cdot 13$, $715 \neq \square + \square$.

Ejercicio

Verifique cuáles de los siguientes números tienen forma $n = x^2 + y^2$. Encuentre x e y correspondiente.

$$n = 160,\ 208,\ 230,\ 351,\ 585,\ 715.$$

$160 = 2^5 \cdot 5$, $160 = 4^2 + 12^2$;

$208 = 2^4 \cdot 13$, $208 = 8^2 + 12^2$;

$230 = 2 \cdot 5 \cdot \boxed{23}$, $230 \neq \square + \square$;

$351 = \boxed{3^3} \cdot 13$, $351 \neq \square + \square$;

$585 = 3^2 \cdot 5 \cdot 13$, $585 = 3^2 + 24^2 = 12^2 + 21^2$;

$715 = 5 \cdot \boxed{11} \cdot 13$, $715 \neq \square + \square$.

Ejercicio

Verifique cuáles de los siguientes números tienen forma $n = x^2 + y^2$. Encuentre x e y correspondiente.

$$n = 160,\ 208,\ 230,\ 351,\ 585,\ 715.$$

$160 = 2^5 \cdot 5$, $160 = 4^2 + 12^2$;

$208 = 2^4 \cdot 13$, $208 = 8^2 + 12^2$;

$230 = 2 \cdot 5 \cdot \boxed{23}$, $230 \neq \square + \square$;

$351 = \boxed{3^3} \cdot 13$, $351 \neq \square + \square$;

$585 = 3^2 \cdot 5 \cdot 13$, $585 = 3^2 + 24^2 = 12^2 + 21^2$;

$715 = 5 \cdot \boxed{11} \cdot 13$, $715 \neq \square + \square$.

Ejercicio

Verifique cuáles de los siguientes números tienen forma $n = x^2 + y^2$. Encuentre x e y correspondiente.

$$n = 160,\ 208,\ 230,\ 351,\ 585,\ 715.$$

$160 = 2^5 \cdot 5$, $160 = 4^2 + 12^2$;

$208 = 2^4 \cdot 13$, $208 = 8^2 + 12^2$;

$230 = 2 \cdot 5 \cdot \boxed{23}$, $230 \neq \square + \square$;

$351 = \boxed{3^3} \cdot 13$, $351 \neq \square + \square$;

$585 = 3^2 \cdot 5 \cdot 13$, $585 = 3^2 + 24^2 = 12^2 + 21^2$;

$715 = 5 \cdot \boxed{11} \cdot 13$, $715 \neq \square + \square$.

Ejercicio

Verifique cuáles de los siguientes números tienen forma $n = x^2 + y^2$. Encuentre x e y correspondiente.

$$n = 160,\ 208,\ 230,\ 351,\ 585,\ 715.$$

$160 = 2^5 \cdot 5$, $160 = 4^2 + 12^2$;

$208 = 2^4 \cdot 13$, $208 = 8^2 + 12^2$;

$230 = 2 \cdot 5 \cdot \boxed{23}$, $230 \neq \square + \square$;

$351 = \boxed{3^3} \cdot 13$, $351 \neq \square + \square$;

$585 = 3^2 \cdot 5 \cdot 13$, $585 = 3^2 + 24^2 = 12^2 + 21^2$;

$715 = 5 \cdot \boxed{11} \cdot 13$, $715 \neq \square + \square$.

Ejercicio

Verifique cuáles de los siguientes números tienen forma $n = x^2 + y^2$. Encuentre x e y correspondiente.

$$n = 160,\ 208,\ 230,\ 351,\ 585,\ 715.$$

$160 = 2^5 \cdot 5$, $160 = 4^2 + 12^2$;

$208 = 2^4 \cdot 13$, $208 = 8^2 + 12^2$;

$230 = 2 \cdot 5 \cdot \boxed{23}$, $230 \neq \square + \square$;

$351 = \boxed{3^3} \cdot 13$, $351 \neq \square + \square$;

$585 = 3^2 \cdot 5 \cdot 13$, $585 = 3^2 + 24^2 = 12^2 + 21^2$;

$715 = 5 \cdot \boxed{11} \cdot 13$, $715 \neq \square + \square$.

Ejercicio

Verifique cuáles de los siguientes números tienen forma $n = x^2 + y^2$. Encuentre x e y correspondiente.

$$n = 160,\ 208,\ 230,\ 351,\ 585,\ 715.$$

$160 = 2^5 \cdot 5$, $\quad 160 = 4^2 + 12^2$;

$208 = 2^4 \cdot 13$, $\quad 208 = 8^2 + 12^2$;

$230 = 2 \cdot 5 \cdot \boxed{23}$, $\quad 230 \neq \square + \square$;

$351 = \boxed{3^3} \cdot 13$, $\quad 351 \neq \square + \square$;

$585 = 3^2 \cdot 5 \cdot 13$, $\quad 585 = 3^2 + 24^2 = 12^2 + 21^2$;

$715 = 5 \cdot \boxed{11} \cdot 13$, $\quad 715 \neq \square + \square$.

¿De dónde viene la identidad de Diofanto?

$$(a^2 + b^2)(c^2 + d^2) = (ac - bd)^2 + (ad + bc)^2. \qquad (*)$$

- De la «Aritmética» de Diofanto ($\sim$ 250 d.C.).
- ¡También de los números complejos!
- **Números complejos**: $z = x + yi$, donde $i^2 = -1$.
- **El conjugado**: $\bar{z} = x - yi$.
  La norma: $N(z) = z\bar{z}$.
- **Ejercicio**:
  1. $z\bar{z} = x^2 + y^2$,
  2. $\overline{zw} = \bar{z} \cdot \overline{w}$,
  3. $N(zw) = N(z)\,N(w)$.
- $(a + bi)(c + di) = (ac - bd) + (ad + bc)\,i$.
  Tomando $N(\cdots)$, se recupera (*).

¿De dónde viene la identidad de Diofanto?

$$(a^2 + b^2)(c^2 + d^2) = (ac - bd)^2 + (ad + bc)^2. \qquad (*)$$

- De la «Aritmética» de Diofanto ($\sim$ 250 d.C.).
- ¡También de los números complejos!
- **Números complejos**: $z = x + yi$, donde $i^2 = -1$.
- **El conjugado**: $\bar{z} = x - yi$.
  La norma: $N(z) = z\bar{z}$.
- **Ejercicio**:
  1. $z\bar{z} = x^2 + y^2$,
  2. $\overline{zw} = \bar{z} \cdot \overline{w}$,
  3. $N(zw) = N(z)\,N(w)$.
- $(a + bi)(c + di) = (ac - bd) + (ad + bc)\,i$.
  Tomando $N(\cdots)$, se recupera (*).

¿De dónde viene la identidad de Diofanto?

$$(a^2 + b^2)(c^2 + d^2) = (ac - bd)^2 + (ad + bc)^2. \qquad (*)$$

- De la «Aritmética» de Diofanto ($\sim$ 250 d.C.).
- ¡También de los números complejos!
- **Números complejos**: $z = x + yi$, donde $i^2 = -1$.
- **El conjugado**: $\bar{z} = x - yi$.
  La norma: $N(z) = z\bar{z}$.
- **Ejercicio**:
  1. $z\bar{z} = x^2 + y^2$,
  2. $\overline{zw} = \bar{z} \cdot \overline{w}$,
  3. $N(zw) = N(z)\,N(w)$.
- $(a + bi)(c + di) = (ac - bd) + (ad + bc)\,i$.
  Tomando $N(\cdots)$, se recupera (*).

¿De dónde viene la identidad de Diofanto?

$$(a^2 + b^2)(c^2 + d^2) = (ac - bd)^2 + (ad + bc)^2. \qquad (*)$$

- De la «Aritmética» de Diofanto ($\sim$ 250 d.C.).
- ¡También de los números complejos!
- **Números complejos**: $z = x + yi$, donde $i^2 = -1$.
- **El conjugado**: $\bar{z} = x - yi$.
  La norma: $N(z) = z\bar{z}$.
- **Ejercicio**:
  1. $z\bar{z} = x^2 + y^2$,
  2. $\overline{zw} = \bar{z} \cdot \overline{w}$,
  3. $N(zw) = N(z)\,N(w)$.
- $(a + bi)(c + di) = (ac - bd) + (ad + bc)\,i$.
  Tomando $N(\cdots)$, se recupera (*).

¿De dónde viene la identidad de Diofanto?

$$(a^2 + b^2)\,(c^2 + d^2) = (ac - bd)^2 + (ad + bc)^2. \qquad (*)$$

- De la «Aritmética» de Diofanto ($\sim$ 250 d.C.).
- ¡También de los números complejos!
- **Números complejos**: $z = x + yi$, donde $i^2 = -1$.
- **El conjugado**: $\bar{z} = x - yi$.
  La norma: $N(z) = z\bar{z}$.
- **Ejercicio**:
  1. $z\bar{z} = x^2 + y^2$,
  2. $\overline{zw} = \bar{z} \cdot \overline{w}$,
  3. $N(zw) = N(z)\,N(w)$.
- $(a + bi)\,(c + di) = (ac - bd) + (ad + bc)\,i$.
  Tomando $N(\cdots)$, se recupera (*).

¿De dónde viene la identidad de Diofanto?

$$(a^2 + b^2)(c^2 + d^2) = (ac - bd)^2 + (ad + bc)^2. \qquad (*)$$

- De la «Aritmética» de Diofanto ($\sim$ 250 d.C.).
- ¡También de los números complejos!
- **Números complejos**: $z = x + yi$, donde $i^2 = -1$.
- **El conjugado**: $\bar{z} = x - yi$.
  La norma: $N(z) = z\bar{z}$.
- **Ejercicio**:
  1. $z\bar{z} = x^2 + y^2$,
  2. $\overline{zw} = \bar{z} \cdot \overline{w}$,
  3. $N(zw) = N(z)\,N(w)$.
- $(a + bi)(c + di) = (ac - bd) + (ad + bc)\,i$.
  Tomando $N(\cdots)$, se recupera (*).

¿De dónde viene la identidad de Diofanto?

$$(a^2 + b^2)(c^2 + d^2) = (ac - bd)^2 + (ad + bc)^2. \qquad (*)$$

- De la «Aritmética» de Diofanto ($\sim$ 250 d.C.).
- ¡También de los números complejos!
- **Números complejos**: $z = x + yi$, donde $i^2 = -1$.
- **El conjugado**: $\bar{z} = x - yi$.
  La norma: $N(z) = z\bar{z}$.
- **Ejercicio**:
  1. $z\bar{z} = x^2 + y^2$,
  2. $\overline{zw} = \bar{z} \cdot \overline{w}$,
  3. $N(zw) = N(z)\,N(w)$.
- $(a + bi)(c + di) = (ac - bd) + (ad + bc)\,i$.
  Tomando $N(\cdots)$, se recupera (*).

Número de representaciones $n = x^2 + y^2$

$$C(n) = \#\{(x, y) \in \mathbb{Z}^2 \mid x^2 + y^2 = n,\ x > 0, y \geq 0\}$$

$$n = p_1^{e_1} \cdots p_s^{e_s}, \quad e_i \text{ par si } p_i \equiv 3\ (4)$$

$$C(n) = \prod_{p_i \equiv 1\ (4)} (e_i + 1)$$

Ejemplo:

- $n = 325$,
- $n = 5^2 \cdot 13$,
- $C(n) = 6$,
- $(x, y) =$
  $(1, 18),\ (6, 17),\ (10, 15),\ (15, 10),\ (17, 6),\ (18, 1)$.

Número de representaciones $n = x^2 + y^2$

$$C(n) = \#\{(x,y) \in \mathbb{Z}^2 \mid x^2 + y^2 = n,\ x > 0, y \geq 0\}$$

$$n = p_1^{e_1} \cdots p_s^{e_s}, \quad e_i \text{ par si } p_i \equiv 3\ (4)$$

$$C(n) = \prod_{p_i \equiv 1\ (4)} (e_i + 1)$$

Ejemplo:

- $n = 325$,
- $n = 5^2 \cdot 13$,
- $C(n) = 6$,
- $(x,y) =$
  $(1,18),\ (6,17),\ (10,15),\ (15,10),\ (17,6),\ (18,1)$.

Tarea

¿Cuántas soluciones enteras tiene $x^2 + y^2 - 16y = 1956$?

Raíces de la unidad complejas y mód p

- $i^2 = -1$, $i^3 = -i$, $i^4 = 1$.
  i es una **cuarta raíz de la unidad**.

Ejercicio: $z = -\frac{1}{2} + \frac{\sqrt{3}}{2}\, i$ es una **raíz cúbica de la unidad**.
Es decir, $z \neq 1$, $z^2 \neq 1$, $z^3 = 1$.

- Analogía con residuos mód p:
  $z^2 \equiv -1 \pmod{p}$ tiene solución si y solo si $p \equiv 1 \pmod{4}$.
  z es una «cuarta raíz de la unidad mód p».

Ejercicio: una raíz cúbica de la unidad mód p existe si y solo si $p \equiv 1 \pmod{3}$.
(Es decir, $z \not\equiv 1$, $z^2 \not\equiv 1$, $z^3 \equiv 1$.)

Ejemplo:
$2^3 \equiv 1 \pmod{7}$, $3^3 \equiv 1 \pmod{13}$, $7^3 \equiv 1 \pmod{19}$, etc.

Raíces de la unidad complejas y mód p

- $i^2 = -1$, $i^3 = -i$, $i^4 = 1$.
  i es una **cuarta raíz de la unidad**.

Ejercicio: $z = -\frac{1}{2} + \frac{\sqrt{3}}{2}\, i$ es una **raíz cúbica de la unidad**.
Es decir, $z \neq 1$, $z^2 \neq 1$, $z^3 = 1$.

- Analogía con residuos mód p:
  $z^2 \equiv -1 \pmod{p}$ tiene solución si y solo si $p \equiv 1 \pmod{4}$.
  z es una «cuarta raíz de la unidad mód p».

Ejercicio: una raíz cúbica de la unidad mód p existe si y solo si $p \equiv 1 \pmod{3}$.
(Es decir, $z \not\equiv 1$, $z^2 \not\equiv 1$, $z^3 \equiv 1$.)

Ejemplo:
$2^3 \equiv 1 \pmod{7}$, $3^3 \equiv 1 \pmod{13}$, $7^3 \equiv 1 \pmod{19}$, etc.

Raíces de la unidad complejas y mód p

- $i^2 = -1$, $i^3 = -i$, $i^4 = 1$.
  i es una **cuarta raíz de la unidad**.

Ejercicio: $z = -\frac{1}{2} + \frac{\sqrt{3}}{2}\, i$ es una **raíz cúbica de la unidad**.
Es decir, $z \neq 1$, $z^2 \neq 1$, $z^3 = 1$.

- Analogía con residuos mód p:
  $z^2 \equiv -1 \pmod{p}$ tiene solución si y solo si $p \equiv 1 \pmod{4}$.
  z es una «cuarta raíz de la unidad mód p».

Ejercicio: una raíz cúbica de la unidad mód p existe si y solo si $p \equiv 1 \pmod{3}$.
(Es decir, $z \not\equiv 1$, $z^2 \not\equiv 1$, $z^3 \equiv 1$.)

Ejemplo:
$2^3 \equiv 1 \pmod{7}$, $3^3 \equiv 1 \pmod{13}$, $7^3 \equiv 1 \pmod{19}$, etc.

Raíces de la unidad complejas y mód p

- $i^2 = -1$, $i^3 = -i$, $i^4 = 1$.
  i es una **cuarta raíz de la unidad**.

Ejercicio: $z = -\frac{1}{2} + \frac{\sqrt{3}}{2}\, i$ es una **raíz cúbica de la unidad**.
Es decir, $z \neq 1$, $z^2 \neq 1$, $z^3 = 1$.

- Analogía con residuos mód p:
  $z^2 \equiv -1 \pmod{p}$ tiene solución si y solo si $p \equiv 1 \pmod{4}$.
  z es una «cuarta raíz de la unidad mód p».

Ejercicio: una raíz cúbica de la unidad mód p existe si y solo si $p \equiv 1 \pmod{3}$.
(Es decir, $z \not\equiv 1$, $z^2 \not\equiv 1$, $z^3 \equiv 1$.)

Ejemplo:
$2^3 \equiv 1 \pmod{7}$, $3^3 \equiv 1 \pmod{13}$, $7^3 \equiv 1 \pmod{19}$, etc.

Raíces de la unidad complejas y mód p

- $i^2 = -1$, $i^3 = -i$, $i^4 = 1$.
  i es una **cuarta raíz de la unidad**.

Ejercicio: $z = -\frac{1}{2} + \frac{\sqrt{3}}{2}\, i$ es una **raíz cúbica de la unidad**.
Es decir, $z \neq 1$, $z^2 \neq 1$, $z^3 = 1$.

- Analogía con residuos mód p:
  $z^2 \equiv -1 \pmod{p}$ tiene solución si y solo si $p \equiv 1 \pmod{4}$.
  z es una «cuarta raíz de la unidad mód p».

Ejercicio: una raíz cúbica de la unidad mód p existe si y solo si $p \equiv 1 \pmod{3}$.
(Es decir, $z \not\equiv 1$, $z^2 \not\equiv 1$, $z^3 \equiv 1$.)

Ejemplo:
$2^3 \equiv 1 \pmod{7}$, $3^3 \equiv 1 \pmod{13}$, $7^3 \equiv 1 \pmod{19}$, etc.

Raíces de la unidad complejas y mód p

- $i^2 = -1$, $i^3 = -i$, $i^4 = 1$.
  i es una **cuarta raíz de la unidad**.

Ejercicio: $z = -\frac{1}{2} + \frac{\sqrt{3}}{2}\, i$ es una **raíz cúbica de la unidad**.
Es decir, $z \neq 1$, $z^2 \neq 1$, $z^3 = 1$.

- Analogía con residuos mód p:
  $z^2 \equiv -1 \pmod{p}$ tiene solución si y solo si $p \equiv 1 \pmod{4}$.
  z es una «cuarta raíz de la unidad mód p».

Ejercicio: una raíz cúbica de la unidad mód p existe si y solo si $p \equiv 1 \pmod{3}$.
(Es decir, $z \not\equiv 1$, $z^2 \not\equiv 1$, $z^3 \equiv 1$.)

Ejemplo:
$2^3 \equiv 1 \pmod{7}$, $3^3 \equiv 1 \pmod{13}$, $7^3 \equiv 1 \pmod{19}$, etc.

¡Gracias!