Ejercicios de la teoría de números

Alexey Beshenov

09/11/2021

Recordatorio de la vez pasada (!)

IWYMIC 2002: Encuentre el número de las soluciones enteras de

$$\frac{1}{x} + \frac{1}{y} = \frac{1}{14}.$$

Dé alguna solución particular.

- La ecuación es equivalente a

$$(x - 14)(y - 14) = 14^2, \quad (x, y) \neq (0, 0).$$

  Por ejemplo, $x = 15$, $y = 14^2 + 14 = 210$ es una solución.
- Tenemos

$$d(14^2) = d(2^2) \cdot d(7^2) = 3 \cdot 3 = 9.$$

  Con signos -1, habrá también 9 divisores.
- Quitando el caso de $(x, y) = (0, 0)$, quedan 17 soluciones.

Recordatorio de la vez pasada (!)

IWYMIC 2002: Encuentre el número de las soluciones enteras de

$$\frac{1}{x} + \frac{1}{y} = \frac{1}{14}.$$

Dé alguna solución particular.

- La ecuación es equivalente a

$$(x - 14)(y - 14) = 14^2, \quad (x, y) \neq (0, 0).$$

  Por ejemplo, $x = 15$, $y = 14^2 + 14 = 210$ es una solución.
- Tenemos

$$d(14^2) = d(2^2) \cdot d(7^2) = 3 \cdot 3 = 9.$$

  Con signos -1, habrá también 9 divisores.
- Quitando el caso de $(x, y) = (0, 0)$, quedan 17 soluciones.

Recordatorio de la vez pasada (!)

IWYMIC 2002: Encuentre el número de las soluciones enteras de

$$\frac{1}{x} + \frac{1}{y} = \frac{1}{14}.$$

Dé alguna solución particular.

- La ecuación es equivalente a

$$(x - 14)(y - 14) = 14^2, \quad (x, y) \neq (0, 0).$$

  Por ejemplo, $x = 15$, $y = 14^2 + 14 = 210$ es una solución.
- Tenemos

$$d(14^2) = d(2^2) \cdot d(7^2) = 3 \cdot 3 = 9.$$

  Con signos -1, habrá también 9 divisores.
- Quitando el caso de $(x, y) = (0, 0)$, quedan 17 soluciones.

Recordatorio de la vez pasada (!)

IWYMIC 2002: Encuentre el número de las soluciones enteras de

$$\frac{1}{x} + \frac{1}{y} = \frac{1}{14}.$$

Dé alguna solución particular.

- La ecuación es equivalente a

$$(x - 14)(y - 14) = 14^2, \quad (x, y) \neq (0, 0).$$

  Por ejemplo, $x = 15$, $y = 14^2 + 14 = 210$ es una solución.
- Tenemos

$$d(14^2) = d(2^2) \cdot d(7^2) = 3 \cdot 3 = 9.$$

  Con signos -1, habrá también 9 divisores.
- Quitando el caso de $(x, y) = (0, 0)$, quedan 17 soluciones.

Recordatorio de la vez pasada (!)

IWYMIC 2002: Encuentre el número de las soluciones enteras de

$$\frac{1}{x} + \frac{1}{y} = \frac{1}{14}.$$

Dé alguna solución particular.

- La ecuación es equivalente a

  $$(x - 14)(y - 14) = 14^2, \quad (x, y) \neq (0, 0).$$

  Por ejemplo, $x = 15$, $y = 14^2 + 14 = 210$ es una solución.
- Tenemos

  $$d(14^2) = d(2^2) \cdot d(7^2) = 3 \cdot 3 = 9.$$

  Con signos -1, habrá también 9 divisores.
- Quitando el caso de $(x, y) = (0, 0)$, quedan 17 soluciones.

Cuadrados

IWIMIC 2005: Encuentre todos los enteros x tales que x e $x + 45$ son cuadrados.

- Escribiendo $x = y^2, y^2 + 45 = z^2$,

$$(y + z)(y - z) = -45 = -3^2 \cdot 5,$$

$$0 < y < z, \quad |y - z| < y + z.$$

- Tres casos:

$$(y + z, y - z) = (9, -5),\ (15, -3),\ (45, -1).$$

  Entonces, $(y, z) = (2, 7),\ (6, 9),\ (22, 23)$.
- Conclusión: $x = 4, 36, 484$.

Cuadrados

IWIMIC 2005: Encuentre todos los enteros x tales que x e $x + 45$ son cuadrados.

- Escribiendo $x = y^2, y^2 + 45 = z^2$,

$$(y + z)(y - z) = -45 = -3^2 \cdot 5,$$

$$0 < y < z, \quad |y - z| < y + z.$$

- Tres casos:

$$(y + z, y - z) = (9, -5),\ (15, -3),\ (45, -1).$$

  Entonces, $(y, z) = (2, 7),\ (6, 9),\ (22, 23)$.
- Conclusión: $x = 4, 36, 484$.

Cuadrados

IWIMIC 2005: Encuentre todos los enteros x tales que x e $x + 45$ son cuadrados.

- Escribiendo $x = y^2$, $y^2 + 45 = z^2$,

$$(y + z)(y - z) = -45 = -3^2 \cdot 5,$$

$$0 < y < z, \quad |y - z| < y + z.$$

- Tres casos:

$$(y + z, y - z) = (9, -5),\ (15, -3),\ (45, -1).$$

  Entonces, $(y, z) = (2, 7),\ (6, 9),\ (22, 23)$.
- Conclusión: $x = 4, 36, 484$.

Cuadrados

IWIMIC 2005: Encuentre todos los enteros x tales que x e $x + 45$ son cuadrados.

- Escribiendo $x = y^2$, $y^2 + 45 = z^2$,

$$(y + z)(y - z) = -45 = -3^2 \cdot 5,$$

$$0 < y < z, \quad |y - z| < y + z.$$

- Tres casos:

$$(y + z, y - z) = (9, -5),\ (15, -3),\ (45, -1).$$

  Entonces, $(y, z) = (2, 7),\ (6, 9),\ (22, 23)$.

- Conclusión: $x = 4, 36, 484$.

Cuadrados

IWIMIC 2005: Encuentre todos los enteros x tales que x e $x + 45$ son cuadrados.

- Escribiendo $x = y^2$, $y^2 + 45 = z^2$,

$$(y + z)(y - z) = -45 = -3^2 \cdot 5,$$

$$0 < y < z, \quad |y - z| < y + z.$$

- Tres casos:

$$(y + z, y - z) = (9, -5),\ (15, -3),\ (45, -1).$$

  Entonces, $(y, z) = (2, 7),\ (6, 9),\ (22, 23)$.

- Conclusión: $x = 4, 36, 484$.

Divisibilidad por un número compuesto

Demuestre que el número

$$f(n) = 23^n + 12^n - 32^n - 3^n$$

es divisible por 35 para todo $n \geq 1$ impar.

- $f(n) \equiv 3^n + 2^n - 2^n - 3^n \pmod 5$
- $f(n) \equiv 2^n + 5^n - 4^n - 3^n$
  $\equiv 2^n + (-2)^n - (-3)^n - 3^n \pmod 7$

Divisibilidad por un número compuesto

Demuestre que el número

$$f(n) = 23^n + 12^n - 32^n - 3^n$$

es divisible por 35 para todo $n \geq 1$ impar.

- $f(n) \equiv 3^n + 2^n - 2^n - 3^n \pmod 5$
- $f(n) \equiv 2^n + 5^n - 4^n - 3^n$
  $\equiv 2^n + (-2)^n - (-3)^n - 3^n \pmod 7$

Divisibilidad por un número compuesto

Demuestre que el número

$$f(n) = 23^n + 12^n - 32^n - 3^n$$

es divisible por 35 para todo $n \geq 1$ impar.

- $f(n) \equiv 3^n + 2^n - 2^n - 3^n \pmod 5$
- $f(n) \equiv 2^n + 5^n - 4^n - 3^n$
  $\equiv 2^n + (-2)^n - (-3)^n - 3^n \pmod 7$

Divisibilidad por un número compuesto

Demuestre que el número

$$f(n) = 23^n + 12^n - 32^n - 3^n$$

es divisible por 35 para todo $n \geq 1$ impar.

- $f(n) \equiv 3^n + 2^n - 2^n - 3^n \pmod 5$
- $f(n) \equiv 2^n + 5^n - 4^n - 3^n$
  $\equiv 2^n + (-2)^n - (-3)^n - 3^n \pmod 7$

Tarea

IWYMIC 2006: Demuestre que el número

$$1596^n + 1000^n - 270^n - 320^n$$

es divisible por 2006 para todo $n \geq 1$ impar.

Contando potencias

- ¿Cuántos números enteros $x \leq N$ son k-ésimas potencias?
- ¿Cuántos números $x \leq N$ no son cuadrados, ni cubos?

- $\lfloor \sqrt[k]{N} \rfloor$ números $1, 2^k, 3^k, 4^k, \ldots$
- Inclusión-exclusión: $f(N) = N - \lfloor \sqrt{N} \rfloor - \lfloor \sqrt[3]{N} \rfloor + \lfloor \sqrt[6]{N} \rfloor$.

Contando potencias

- ¿Cuántos números enteros $x \leq N$ son k-ésimas potencias?
- ¿Cuántos números $x \leq N$ no son cuadrados, ni cubos?

- $\lfloor \sqrt[k]{N} \rfloor$ números $1, 2^k, 3^k, 4^k, \ldots$
- Inclusión-exclusión: $f(N) = N - \lfloor \sqrt{N} \rfloor - \lfloor \sqrt[3]{N} \rfloor + \lfloor \sqrt[6]{N} \rfloor$.

Contando potencias

- ¿Cuántos números enteros $x \leq N$ son k-ésimas potencias?
- ¿Cuántos números $x \leq N$ no son cuadrados, ni cubos?

- $\lfloor \sqrt[k]{N} \rfloor$ números $1, 2^k, 3^k, 4^k, \ldots$
- Inclusión-exclusión: $f(N) = N - \lfloor \sqrt{N} \rfloor - \lfloor \sqrt[3]{N} \rfloor + \lfloor \sqrt[6]{N} \rfloor$.

Contando potencias

- ¿Cuántos números enteros $x \leq N$ son k-ésimas potencias?
- ¿Cuántos números $x \leq N$ no son cuadrados, ni cubos?

- $\lfloor \sqrt[k]{N} \rfloor$ números $1, 2^k, 3^k, 4^k, \ldots$
- Inclusión-exclusión: $f(N) = N - \lfloor \sqrt{N} \rfloor - \lfloor \sqrt[3]{N} \rfloor + \lfloor \sqrt[6]{N} \rfloor$.

Contando potencias (cont.)

IWYMIC 2005: Consideremos la sucesión de los números enteros que no son cuadrados ni cubos:

$$2, 3, 5, 6, 7, 10, 11, 12, 13, 14, \ldots$$

Encuentre el término número 1000.

- Buscamos $f(N) = 1000$ para $f(N) = N - \lfloor \sqrt{N} \rfloor - \lfloor \sqrt[3]{N} \rfloor + \lfloor \sqrt[6]{N} \rfloor$.
- $f(1000) = 1000 - 31 - 10 + 3 = 962$
- $f(1050) = 1050 - 32 - 10 + 3 = 1011$
- $f(1039) = 1039 - 32 - 10 + 3 = 1000$ (prueba y error)

Contando potencias (cont.)

IWYMIC 2005: Consideremos la sucesión de los números enteros que no son cuadrados ni cubos:

$$2, 3, 5, 6, 7, 10, 11, 12, 13, 14, \ldots$$

Encuentre el término número 1000.

- Buscamos $f(N) = 1000$ para $f(N) = N - \lfloor \sqrt{N} \rfloor - \lfloor \sqrt[3]{N} \rfloor + \lfloor \sqrt[6]{N} \rfloor$.
- $f(1000) = 1000 - 31 - 10 + 3 = 962$
- $f(1050) = 1050 - 32 - 10 + 3 = 1011$
- $f(1039) = 1039 - 32 - 10 + 3 = 1000$ (prueba y error)

Contando potencias (cont.)

IWYMIC 2005: Consideremos la sucesión de los números enteros que no son cuadrados ni cubos:

$$2, 3, 5, 6, 7, 10, 11, 12, 13, 14, \ldots$$

Encuentre el término número 1000.

- Buscamos $f(N) = 1000$ para $f(N) = N - \lfloor \sqrt{N} \rfloor - \lfloor \sqrt[3]{N} \rfloor + \lfloor \sqrt[6]{N} \rfloor$.
- $f(1000) = 1000 - 31 - 10 + 3 = 962$
- $f(1050) = 1050 - 32 - 10 + 3 = 1011$
- $f(1039) = 1039 - 32 - 10 + 3 = 1000$ (prueba y error)

Contando potencias (cont.)

IWYMIC 2005: Consideremos la sucesión de los números enteros que no son cuadrados ni cubos:

$$2, 3, 5, 6, 7, 10, 11, 12, 13, 14, \ldots$$

Encuentre el término número 1000.

- Buscamos $f(N) = 1000$ para $f(N) = N - \lfloor \sqrt{N} \rfloor - \lfloor \sqrt[3]{N} \rfloor + \lfloor \sqrt[6]{N} \rfloor$.
- $f(1000) = 1000 - 31 - 10 + 3 = 962$
- $f(1050) = 1050 - 32 - 10 + 3 = 1011$
- $f(1039) = 1039 - 32 - 10 + 3 = 1000$ (prueba y error)

Contando potencias (cont.)

IWYMIC 2005: Consideremos la sucesión de los números enteros que no son cuadrados ni cubos:

$$2, 3, 5, 6, 7, 10, 11, 12, 13, 14, \ldots$$

Encuentre el término número 1000.

- Buscamos $f(N) = 1000$ para $f(N) = N - \lfloor \sqrt{N} \rfloor - \lfloor \sqrt[3]{N} \rfloor + \lfloor \sqrt[6]{N} \rfloor$.
- $f(1000) = 1000 - 31 - 10 + 3 = 962$
- $f(1050) = 1050 - 32 - 10 + 3 = 1011$
- $f(1039) = 1039 - 32 - 10 + 3 = 1000$ (prueba y error)

Contando potencias (cont.)

IWYMIC 2005: Consideremos la sucesión de los números enteros que no son cuadrados ni cubos:

$$2, 3, 5, 6, 7, 10, 11, 12, 13, 14, \ldots$$

Encuentre el término número 1000.

- Buscamos $f(N) = 1000$ para $f(N) = N - \lfloor \sqrt{N} \rfloor - \lfloor \sqrt[3]{N} \rfloor + \lfloor \sqrt[6]{N} \rfloor$.
- $f(1000) = 1000 - 31 - 10 + 3 = 962$
- $f(1050) = 1050 - 32 - 10 + 3 = 1011$
- $f(1039) = 1039 - 32 - 10 + 3 = 1000$ (prueba y error)

Tarea

- ¿Cuántos números $x \leq N$ no son cuadrados, ni cubos, ni quintas potencias?
- ¿Cuál es el término número 4321 en la sucesión correspondiente?

Sumas de dos cuadrados

Resuelve la congruencia $x^2 \equiv -1 \pmod{p}$ para $p = 5, 7, 11, 13$.

- $(\pm 2)^2 = 4 \equiv -1 \pmod{5}$.
- $(\pm 1)^2 = 1, (\pm 2)^2 = 4, (\pm 3)^2 \equiv 2$ son todos los cuadrados mód 7.
  Otra opción: usando una raíz primitiva 3:

$$\underline{3^0 \equiv 1}, 3, \underline{3^2 \equiv 2}, 3^3 \equiv 6, \underline{3^4 \equiv 4}, 3^5 \equiv 5.$$

- $(\pm 1)^2 = 1, (\pm 2)^2 = 4, (\pm 3)^2 = 9, (\pm 4)^2 \equiv 5, (\pm 5)^2 \equiv 3$ son todos los cuadrados mód 11.
- $(\pm 5)^2 \equiv -1 \pmod{13}$.

Sumas de dos cuadrados

Resuelve la congruencia $x^2 \equiv -1 \pmod{p}$ para $p = 5, 7, 11, 13$.

- $(\pm 2)^2 = 4 \equiv -1 \pmod{5}$.
- $(\pm 1)^2 = 1, (\pm 2)^2 = 4, (\pm 3)^2 \equiv 2$ son todos los cuadrados mód 7.
  Otra opción: usando una raíz primitiva 3:

$$\underline{3^0 \equiv 1}, 3, \underline{3^2 \equiv 2}, 3^3 \equiv 6, \underline{3^4 \equiv 4}, 3^5 \equiv 5.$$

- $(\pm 1)^2 = 1, (\pm 2)^2 = 4, (\pm 3)^2 = 9, (\pm 4)^2 \equiv 5, (\pm 5)^2 \equiv 3$ son todos los cuadrados mód 11.
- $(\pm 5)^2 \equiv -1 \pmod{13}$.

Sumas de dos cuadrados

Resuelve la congruencia $x^2 \equiv -1 \pmod{p}$ para $p = 5, 7, 11, 13$.

- $(\pm 2)^2 = 4 \equiv -1 \pmod{5}$.
- $(\pm 1)^2 = 1, (\pm 2)^2 = 4, (\pm 3)^2 \equiv 2$ son todos los cuadrados mód 7.
  Otra opción: usando una raíz primitiva 3:

$$\underline{3^0 \equiv 1}, 3, \underline{3^2 \equiv 2}, 3^3 \equiv 6, \underline{3^4 \equiv 4}, 3^5 \equiv 5.$$

- $(\pm 1)^2 = 1, (\pm 2)^2 = 4, (\pm 3)^2 = 9, (\pm 4)^2 \equiv 5, (\pm 5)^2 \equiv 3$ son todos los cuadrados mód 11.
- $(\pm 5)^2 \equiv -1 \pmod{13}$.

Sumas de dos cuadrados

Resuelve la congruencia $x^2 \equiv -1 \pmod{p}$ para $p = 5, 7, 11, 13$.

- $(\pm 2)^2 = 4 \equiv -1 \pmod{5}$.
- $(\pm 1)^2 = 1, (\pm 2)^2 = 4, (\pm 3)^2 \equiv 2$ son todos los cuadrados mód 7.
  Otra opción: usando una raíz primitiva 3:

$$\underline{3^0 \equiv 1}, 3, \underline{3^2 \equiv 2}, 3^3 \equiv 6, \underline{3^4 \equiv 4}, 3^5 \equiv 5.$$

- $(\pm 1)^2 = 1, (\pm 2)^2 = 4, (\pm 3)^2 = 9, (\pm 4)^2 \equiv 5, (\pm 5)^2 \equiv 3$ son todos los cuadrados mód 11.
- $(\pm 5)^2 \equiv -1 \pmod{13}$.

Sumas de dos cuadrados

Resuelve la congruencia $x^2 \equiv -1 \pmod{p}$ para $p = 5, 7, 11, 13$.

- $(\pm 2)^2 = 4 \equiv -1 \pmod{5}$.
- $(\pm 1)^2 = 1, (\pm 2)^2 = 4, (\pm 3)^2 \equiv 2$ son todos los cuadrados mód 7.
  Otra opción: usando una raíz primitiva 3:

$$\underline{3^0 \equiv 1}, 3, \underline{3^2 \equiv 2}, 3^3 \equiv 6, \underline{3^4 \equiv 4}, 3^5 \equiv 5.$$

- $(\pm 1)^2 = 1, (\pm 2)^2 = 4, (\pm 3)^2 = 9, (\pm 4)^2 \equiv 5, (\pm 5)^2 \equiv 3$ son todos los cuadrados mód 11.
- $(\pm 5)^2 \equiv -1 \pmod{13}$.

Sumas de dos cuadrados

Resuelve la congruencia $x^2 \equiv -1 \pmod{p}$ para $p = 5, 7, 11, 13$.

- $(\pm 2)^2 = 4 \equiv -1 \pmod{5}$.
- $(\pm 1)^2 = 1, (\pm 2)^2 = 4, (\pm 3)^2 \equiv 2$ son todos los cuadrados mód 7.
  Otra opción: usando una raíz primitiva 3:

$$\underline{3^0 \equiv 1}, 3, \underline{3^2 \equiv 2}, 3^3 \equiv 6, \underline{3^4 \equiv 4}, 3^5 \equiv 5.$$

- $(\pm 1)^2 = 1, (\pm 2)^2 = 4, (\pm 3)^2 = 9, (\pm 4)^2 \equiv 5, (\pm 5)^2 \equiv 3$ son todos los cuadrados mód 11.
- $(\pm 5)^2 \equiv -1 \pmod{13}$.

Sumas de dos cuadrados (cont.)

Para un primo impar p, demuestre que $x^2 \equiv -1 \pmod{p}$ tiene soluciones si y solo si $p \equiv 1 \pmod{4}$.

* Sugerencia: *existe una raíz primitiva a tal que $a, a^2, \ldots, a^{p-2}, a^{p-1} \equiv 1$ son todos los residuos no nulos mód p.*

- $x^2 \equiv -1, x^3 \equiv -x \not\equiv 1, x^4 \equiv 1$.
- Pequeño teorema de Fermat: $x^{p-1} \equiv 1$.
- $p - 1 = 4n + r$, donde $0 \leq r < 4$.
- $1 = x^{p-1} = (x^4)^n \cdot x^r = x^r$, entonces $r = 0$.
- Si $4 \mid p - 1$, funciona $x = a^{\frac{p-1}{4}}$.

Sumas de dos cuadrados (cont.)

Para un primo impar p, demuestre que $x^2 \equiv -1 \pmod{p}$ tiene soluciones si y solo si $p \equiv 1 \pmod{4}$.

* Sugerencia: *existe una raíz primitiva a tal que $a, a^2, \ldots, a^{p-2}, a^{p-1} \equiv 1$ son todos los residuos no nulos mód p.*

- $x^2 \equiv -1, x^3 \equiv -x \not\equiv 1, x^4 \equiv 1$.
- Pequeño teorema de Fermat: $x^{p-1} \equiv 1$.
- $p - 1 = 4n + r$, donde $0 \leq r < 4$.
- $1 = x^{p-1} = (x^4)^n \cdot x^r = x^r$, entonces $r = 0$.
- Si $4 \mid p - 1$, funciona $x = a^{\frac{p-1}{4}}$.

Sumas de dos cuadrados (cont.)

Para un primo impar p, demuestre que $x^2 \equiv -1 \pmod{p}$ tiene soluciones si y solo si $p \equiv 1 \pmod{4}$.

* Sugerencia: *existe una raíz primitiva a tal que $a, a^2, \ldots, a^{p-2}, a^{p-1} \equiv 1$ son todos los residuos no nulos mód p.*

- $x^2 \equiv -1, x^3 \equiv -x \not\equiv 1, x^4 \equiv 1$.
- Pequeño teorema de Fermat: $x^{p-1} \equiv 1$.
- $p - 1 = 4n + r$, donde $0 \leq r < 4$.
- $1 = x^{p-1} = (x^4)^n \cdot x^r = x^r$, entonces $r = 0$.
- Si $4 \mid p - 1$, funciona $x = a^{\frac{p-1}{4}}$.

Sumas de dos cuadrados (cont.)

Para un primo impar p, demuestre que $x^2 \equiv -1 \pmod{p}$ tiene soluciones si y solo si $p \equiv 1 \pmod{4}$.

* Sugerencia: *existe una raíz primitiva a tal que $a, a^2, \ldots, a^{p-2}, a^{p-1} \equiv 1$ son todos los residuos no nulos mód p.*

- $x^2 \equiv -1, x^3 \equiv -x \not\equiv 1, x^4 \equiv 1$.
- Pequeño teorema de Fermat: $x^{p-1} \equiv 1$.
- $p - 1 = 4n + r$, donde $0 \leq r < 4$.
- $1 = x^{p-1} = (x^4)^n \cdot x^r = x^r$, entonces $r = 0$.
- Si $4 \mid p - 1$, funciona $x = a^{\frac{p-1}{4}}$.

Sumas de dos cuadrados (cont.)

Para un primo impar p, demuestre que $x^2 \equiv -1 \pmod{p}$ tiene soluciones si y solo si $p \equiv 1 \pmod{4}$.

* Sugerencia: *existe una raíz primitiva a tal que $a, a^2, \ldots, a^{p-2}, a^{p-1} \equiv 1$ son todos los residuos no nulos mód p.*

- $x^2 \equiv -1, x^3 \equiv -x \not\equiv 1, x^4 \equiv 1$.
- Pequeño teorema de Fermat: $x^{p-1} \equiv 1$.
- $p - 1 = 4n + r$, donde $0 \leq r < 4$.
- $1 = x^{p-1} = (x^4)^n \cdot x^r = x^r$, entonces $r = 0$.
- Si $4 \mid p - 1$, funciona $x = a^{\frac{p-1}{4}}$.

Sumas de dos cuadrados (cont.)

Para un primo impar p, demuestre que $x^2 \equiv -1 \pmod{p}$ tiene soluciones si y solo si $p \equiv 1 \pmod{4}$.

* Sugerencia: *existe una raíz primitiva a tal que $a, a^2, \ldots, a^{p-2}, a^{p-1} \equiv 1$ son todos los residuos no nulos mód p.*

- $x^2 \equiv -1, x^3 \equiv -x \not\equiv 1, x^4 \equiv 1$.
- Pequeño teorema de Fermat: $x^{p-1} \equiv 1$.
- $p - 1 = 4n + r$, donde $0 \leq r < 4$.
- $1 = x^{p-1} = (x^4)^n \cdot x^r = x^r$, entonces $r = 0$.
- Si $4 \mid p - 1$, funciona $x = a^{\frac{p-1}{4}}$.

Sumas de dos cuadrados (cont.)

Para un primo impar p, demuestre que $x^2 \equiv -1 \pmod{p}$ tiene soluciones si y solo si $p \equiv 1 \pmod{4}$.

* Sugerencia: *existe una raíz primitiva a tal que $a, a^2, \ldots, a^{p-2}, a^{p-1} \equiv 1$ son todos los residuos no nulos mód p.*

- $x^2 \equiv -1, x^3 \equiv -x \not\equiv 1, x^4 \equiv 1$.
- Pequeño teorema de Fermat: $x^{p-1} \equiv 1$.
- $p - 1 = 4n + r$, donde $0 \leq r < 4$.
- $1 = x^{p-1} = (x^4)^n \cdot x^r = x^r$, entonces $r = 0$.
- Si $4 \mid p - 1$, funciona $x = a^{\frac{p-1}{4}}$.

Sumas de dos cuadrados (cont.) / Tarea

Sea p un primo impar. Demuestre que $x^2 + y^2 \equiv 0 \pmod{p}$ tiene soluciones no triviales $(x, y) \not\equiv (0, 0) \pmod{p}$ si y solo si $p \equiv 1 \pmod{4}$.

Sumas de dos cuadrados (cont.) / Tarea

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

Tarea

Verifique si $x^2 + y^2 - 16y = 2020$ tiene soluciones.
* Difícil: ¿Cuántas son en total?

Lectura adicional: «El Libro de las Demostraciones», cap. 4, Representación de enteros como suma de dos cuadrados.