Algunos ejercicios de la teoría de números elemental

Alexey Beshenov (cadadr@gmail.com)

21 de septiembre de 2021

Los ejercicios de esta hoja usan los siguientes conceptos de la teoría de números elemental: divisibilidad, mcd, identidad de Bézout, factorización en números primos, congruencias mód n, función ϕ de Euler.

Ejercicios para hacer en vivo

Problema 0.

a) Encuentre el mínimo número positivo n de la forma $30a + 105b$ para $a, b \in \mathbb{Z}$.
¿Cuáles son los a y b correspondientes? ¿Son únicos?

b) Calcule $5^{2021} \pmod{13}$.

c) Para $N = 105$, ¿cuántos números $0 \le x < N$ son invertibles módulo N?

d) Para $n = 2, 3, 4, 5, 6$, ¿cuántos números $0 \le x < 13$ satisfacen $x \equiv y^n \pmod{13}$ para algún $y \in \mathbb{Z}$?

Solución. En a), tenemos $\mathrm{mcd}(30, 105) = 15$, así que $30a + 105b$ es divisible por 15. Esto demuestra que $30a + 105b \ge 15$, cuando $30a + 105b$ es positivo. El algoritmo de Euclides nos da la identidad de Bézout con $(a, b) = (-3, 1)$:

$$30 \cdot (-3) + 105 \cdot 1 = 15.$$

Los coeficientes a, b no son para nada únicos: por ejemplo, en lugar de $(-3, 1)$ funcionaría $(4, -1)$. Véase el problema 12.

En b), notamos que $5^2 = 25 \equiv 12 \equiv -1 \pmod{13}$. Luego,

$$5^3 \equiv -5,\ 5^4 \equiv 1,\ \ldots,\ 5^{2021} = 5 \cdot (5^4)^{505} \equiv 5.$$

En c), el número de los restos invertibles mód n es la función de Euler $\phi(n)$. Luego $\phi(105) = \phi(3)\,\phi(5)\,\phi(7) = 2 \cdot 4 \cdot 6 = 48$.

En d), podemos usar el siguiente resultado poderoso: para todo primo p existe un número $x \in \mathbb{Z}$ (llamado una **raíz primitiva mód** p) tal que las potencias

$$1, x, x^2, \ldots, x^{p-2}$$

representan los diferentes restos no nulos módulo p.

En general no hay una manera sencilla de encontrar el x en cuestión, pero para $p = 13$ funciona $x = 2$:

$$2^0 \equiv 1,\ 2^1 \equiv 2,\ 2^2 \equiv 4,\ 2^3 \equiv 8,\ 2^4 \equiv 3,\ 2^5 \equiv 6,\ 2^6 \equiv 12,\ 2^7 \equiv 11,\ 2^8 \equiv 9,\ 2^9 \equiv 5,\ 2^{10} \equiv 10,\ 2^{11} \equiv 7.$$

Luego los cuadrados no nulos mód 13 son las potencias pares de 2:

$$1 \equiv 2^0,\ 3 \equiv 2^4,\ 4 = 2^2,\ 9 \equiv 2^8,\ 10 \equiv 2^{10},\ 12 \equiv 2^6.$$

De la misma manera, las cuartas potencias no nulas son

$$1 \equiv 2^0,\ 3 \equiv 2^4,\ 9 \equiv 2^8.$$

Los cubos serán las potencias de 2 divisibles por 3:

$$1 \equiv 2^0,\ 5 \equiv 2^9,\ 8 = 2^3,\ 12 \equiv 2^6.$$

Aquí las sextas potencias son 1 y $12 \equiv -1$.

Lo más interesante sucede con las quintas potencias. Tenemos $2^5 = 6$, y de hecho 6 es otra raíz primitiva: las potencias de 6 recorren todos los restos no nulos mód 13. Esto significa que cualquier resto es una quinta potencia:

$$2 \equiv 6^5,\ 3 \equiv 9^5,\ 4 \equiv 10^5,\ 5 \equiv 5^5,\ 6 \equiv 2^5,\ 7 \equiv 11^5,\ 8 \equiv 8^5,\ 9 \equiv 3^5,\ 10 \equiv 4^5,\ 11 \equiv 7^5,\ 12 \equiv 12^5.$$

Esto se debe al hecho de que $\mathrm{mcd}(5, 12) = 1$. (¿Por qué?) □

Problema 1. Si $\mathrm{mcd}(a, b) = \mathrm{mcd}(c, d) = 1$ y $\frac{a}{b} + \frac{c}{d}$ es un número entero, demuestre que necesariamente $b = \pm d$.

Solución. Tenemos

$$\frac{a}{b} + \frac{c}{d} = \frac{ad + bc}{bd},$$

donde

$$ad + bc = bde.$$

Ahora $ad = b(de - c)$ y $\mathrm{mcd}(a, b) = 1$, así que $b \mid d$. De manera similar se ve que $d \mid b$. □

Problema 2. El teorema de Wilson afirma que $(p-1)! \equiv -1 \pmod{p}$ para p primo. Demuestre que $(n-1)! \equiv 0 \pmod{n}$ si $n \geq 6$ es compuesto.

Solución. Supongamos que $n = ab$, donde $1 < a, b < n$. Entre los números $2, 3, 4, \ldots, n-1$ necesariamente aparecen a y b. Si $a \neq b$, esto nos permite concluir que $n \mid (n-1)!$. En el caso especial de $a = b$, tenemos $n = a^2$. Notamos que $2a < a^2$ para $a > 2$, así que entre los números $2, 3, 4, \ldots, a^2 - 1$ aparecen a y $2a$. Luego, $a^2 \mid (a^2 - 1)!$ para $a > 2$. □

Problema 3.

a) Demuestre que $\mathrm{mcd}(a, a + b) \mid b$.

b) Si $\mathrm{mcd}(a, b) = 1$, demuestre que $\mathrm{mcd}(a + b, a - b) = 1$ o 2.
   En particular, calcule $\mathrm{mcd}(a + 1, a - 1)$.

Solución. En parte a), si $d = \gcd(a, a + b)$, entonces $d \mid a$ y $d \mid a + b$, y luego $d \mid b$.

En la parte b), tenemos $d \mid (a + b)$ y $d \mid (a - b)$, así que $d \mid 2a$ y $d \mid 2b$. Puesto que a y b son coprimos, podemos concluir que $d = 1$ o 2.

En particular, no es difícil calcular que

$$\mathrm{mcd}(a - 1, a + 1) = \begin{cases} 1, & \text{si } a \text{ es par,} \\ 2, & \text{si } a \text{ es impar.} \end{cases}$$

□

Problema 4 (IWYMIC 2019 Individual contest)**.** Encuentre el mínimo n tal que $x = 55n^3$ que tiene 55 divisores $1 \leq d \leq x$, $d \mid x$.

Solución. Vamos a denotar por $d(x)$ la función del número de divisores. Tenemos $d(p^e) = e+1$. Esta función es multiplicativa, así que

$$d(p_1^{e_1} \cdots p_s^{e_s}) = (e_1+1)\cdots(e_s+1).$$

En nuestro caso, buscamos n tal que $d(55\,n^3) = 55$. Puesto que $55 = 5 \cdot 11$, no tenemos muchas opciones: $x = p^4 q^{10}$ o $p^{10} q^4$, donde $p = 5$, $q = 11$. El número más pequeño es visiblemente $5^{10} \cdot 11^4$. Sustituyendo $n = 5^a \cdot 11^b$, calculamos de

$$5^{10} \cdot 11^4 = 55\,n^3 = 5^{3a+1} \cdot 11^{3b+1}$$

que $n = 5^3 \cdot 11 = 1375$. □

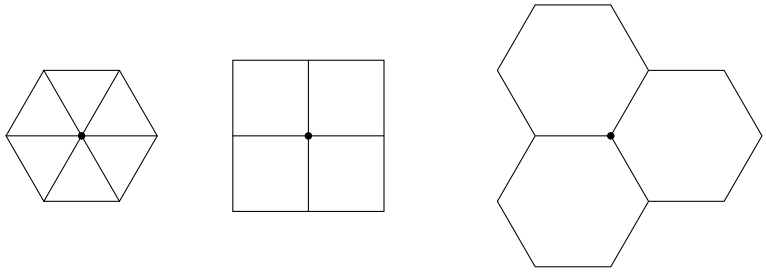
Problema 5 (IWYMIC 2019 Team contest). p_1, p_2, p_3 son primos tales que

$$p_1 p_2 p_3 = p_1 + p_2 + p_3 + 1007.$$

Encuentre p_1, p_2, p_3.

Solución. Reduciendo mód 2, primero notamos que necesariamente dos de estos primos son pares: $p_1 = p_2 = 2$. Pongamos $p_3 = p$. Nos queda nada más $4p = p + 1011$, de donde $p = 337$. Este número es primo. □

Problema 6. Se fija un punto en el plano y se consideran unas copias de n-ágono regular, tratando de colocarlas alrededor del punto. Demuestre que esto es posible solamente con 6 triángulos, o 3 cuadrados, o 6 hexágonos, como en el dibujo de abajo:



Sugerencia: si N es el número de n-ágonos, entonces $N \cdot (n-2)\,\frac{\pi}{n} = 2\pi$. (¿Por qué?)

Solución. Un ángulo del n-ágono regular mide $(n-2)\,\frac{\pi}{n}$. Por otra parte, la suma de N estos ángulos alrededor del punto debe ser 2π. Tenemos entonces $N \cdot (n-2)\,\frac{\pi}{n} = 2\pi$. Esto nos deja la ecuación $N = \frac{2n}{n-2}$. Hay que ver que $(n, N) = (3,6), (4,4), (6,3)$ son las únicas soluciones. La función $f(n) = \frac{2n}{n-2}$ decrece para $n \geq 3$, y además $f(n) \xrightarrow{n\to\infty} 2$. Calculamos que

$$f(3) = 6, \quad f(4) = 4, \quad f(5) = \frac{10}{3}, \quad f(6) = 3, \quad f(7) = \frac{14}{5} < 3,$$

así que $2 < f(n) < 3$ para $n \geq 7$. Entonces, los únicos valores enteros son $f(3) = 6$, $f(4) = 4$, $f(6) = 3$.

Una manera más aritmética de resolver la ecuación $N = \frac{2n}{n-2}$ es notar que esta es equivalente a la ecuación $(N-2)\,(n-2) = 4$. □

Problema 7. Demuestre que si $a^n - 1$ es primo, entonces $a = 2$ y n es primo.

Solución. Si $p \mid n$ para un primo impar p, entonces escribiendo $m = n/p$, se obtiene

$$a^n - 1 = (a^m)^p + 1^p = (a^m + 1)\,(a^{m(p-1)} + a^{m(p-2)} + \cdots + 1),$$

y necesariamente $a = 2$ y $n = p$.

Un lema muy útil: para $a > 2$ tenemos $a^m - 1 \mid a^n - 1$ si y solamente si $m \mid n$ (¡demuéstrelo!) □

Comentario. Los primos de la forma $2^p - 1$ se conocen como los **primos de Mersenne**; su infinitud es una conjetura abierta. Muchos de los números $2^p - 1$ son compuestos, el primero siendo $2^{11} - 1 = 23 \cdot 89$.

$2^2 - 1$: primo $= 3$
$2^3 - 1$: primo $= 7$
$2^5 - 1$: primo $= 31$
$2^7 - 1$: primo $= 127$
$2^{11} - 1$: compuesto $= 23 \cdot 89$
$2^{13} - 1$: primo $= 8191$
$2^{17} - 1$: primo $= 131071$
$2^{19} - 1$: primo $= 524287$
$2^{23} - 1$: compuesto $= 47 \cdot 178481$
$2^{29} - 1$: compuesto $= 233 \cdot 1103 \cdot 2089$
$2^{31} - 1$: primo $= 2147483647$
$2^{37} - 1$: compuesto $= 223 \cdot 616318177$
$2^{41} - 1$: compuesto $= 13367 \cdot 164511353$
$\dots$
$2^{61} - 1$: primo $= 2305843009213693951$
$2^{67} - 1$: compuesto $= 193707721 \cdot 761838257287$
$\dots$

Problema 8. Demuestre que si $a^n + 1$ es primo, entonces a es par y $n = 2^k$ es una potencia de 2.

Comentario. Los primos de la forma $2^{2^k} + 1$ se conocen como los **primos de Fermat**. Su finitud es una conjetura abierta. El primer número compuesto de esta forma es $2^{2^5} + 1 = 641 \cdot 6700417$ (dos factores primos). Note que estos números crecen muy rápido con k.

$2^{2^0} + 1$: primo $= 3$
$2^{2^1} + 1$: primo $= 5$
$2^{2^2} + 1$: primo $= 17$
$2^{2^3} + 1$: primo $= 257$
$2^{2^4} + 1$: primo $= 65537$
$2^{2^5} + 1$: compuesto $= 641 \cdot 6700417$
$2^{2^6} + 1$: compuesto $= 274177 \cdot 67280421310721$
$2^{2^7} + 1$: compuesto $= 59649589127497217 \cdot 5704689200685129054721$

Fermat conjeturó (demasiado optimísticamente) que los números de la forma $2^{2^k} + 1$ son primos, pero Euler descubrió que $641 \mid (2^{2^5} + 1)$. De hecho, parece que para todo $k \geq 5$ los números $2^{2^k} + 1$ son compuestos.

Problema 9.

a) Para $a \neq 0$ y $m \neq n$ calcule $\text{mcd}(a^{2^m} + 1, a^{2^n} + 1)$.

b) Concluya que los números $2^2 + 1$, $2^{2^2} + 1$, $2^{2^3} + 1$, … son coprimos por pares.

Ejercicios para hacer en casa

Problema 10.

a) Demuestre que si n es impar, entonces $8 \mid (n^2-1)$. Además, si $3 \nmid n$, entonces $6 \mid (n^2-1)$.

b) Demuestre que para todo n, se tiene $30 \mid (n^5-n)$ y $42 \mid (n^7-n)$.

Problema 11. Sean a, b, c números enteros.

a) Demuestre que la ecuación

$$ax + by = c$$

tiene una solución entera (x, y) si y solamente si $\mathrm{mcd}(a, b) \mid c$.

b) (*) Si (x_0, y_0) es una solución, demuestre que todas las soluciones tienen forma

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

para $d = \mathrm{mcd}(a, b)$ y $t \in \mathbb{Z}$.

Problema 12. Para un entero n y un parámetro natural $k = 0, 1, 2, \ldots$, definamos

$$\sigma_k(n) = \sum_{\substack{1 \le d \le n \\ d \mid n}} d^k.$$

a) Demuestre que $\sigma_k(mn) = \sigma_k(m)\,\sigma_k(n)$ para $\mathrm{mcd}(m, n) = 1$.

b) Para $n = p_1^{e_1} \cdots p_s^{e_s}$, deduzca una fórmula para $\sigma_k(n)$.

Problema 13. Como un caso particular del ejercicio anterior, consideremos el número de divisores

$$d(n) = \sigma_0(n) = \#\{1 \le d \le n \mid d \mid n\}.$$

Encuentre los números tales que $d(n) = n/3$ y $n = d(n)^2$.

Problema 14 (IWYMIC 2019 Individual contest)**.** Encuentre todas las soluciones enteras (m, n) de la ecuación

$$\frac{m^2 + mn + n^2}{m + 2n} = \frac{13}{3}.$$

Solución. Para algún entero $a \neq 0$ se tiene

$$\begin{aligned} m^2 + mn + n^2 &= 13a, \\ m + 2n &= 3a. \end{aligned}$$

Podemos, por ejemplo, sustituir $m = 3a - 2n$ en la primera ecuación, y analizar la ecuación cuadrática en n:

$$\begin{aligned} (3a - 2n)^2 + (3a - 2n)\,n + n^2 &= 13a, \\ 3n^2 - 9an + (9a^2 - 13a) &= 0. \end{aligned}$$

De aquí calculamos el discriminante

$$D = 156\,a - 27\,a^2 = 27a\left(\frac{52}{9} - a\right).$$

Esto nos deja con la condición

$$0 < a < \frac{52}{9} < 6 \Longrightarrow a = 1, 2, 3, 4, 5.$$

Antes de sustituir estos a en el sistema de ecuaciones, hay varias formas de reducir el trabajo. Por ejemplo, al elevar al cuadrado la segunda ecuación, nos queda el sistema

$$\begin{aligned} m^2 + mn + n^2 &= 13a, \\ m^2 + 4mn + 4n^2 &= 9a^2. \end{aligned}$$

De aquí, restando,

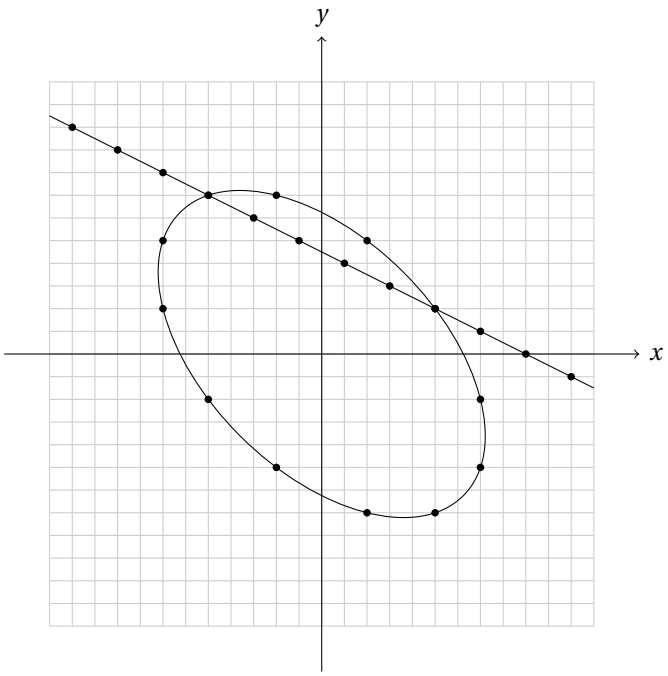
$$3mn + 3n^2 = 9a^2 - 13a,$$

lo que implica que $3 \mid a$. Entonces, la única opción es $a = 3$, y luego $m + 2n = 9$. En términos de (m, n), habrá exactamente dos soluciones: $(-5, 7)$ y $(5, 2)$.

* * *

Para explicar qué está pasando y poner este problema en algún contexto, la ecuación $x^2 + xy + y^2 = 13a$ define una elipse para $a > 0$, mientras que $x + 2y = 3a$ define una recta.

- Para $a = 0$ la elipse se degenera en un punto, que es el origen, y la recta pasa por el origen.
- Para $0 < a < \frac{52}{9}$, la recta tendrá exactamente dos puntos de intersección con la elipse.
- Para $a = \frac{52}{9}$ habrá una tangencia entre la elipse y la recta.
- Para $a > \frac{52}{9}$ no habrá intersecciones entre la recta y la elipse.



La elipse $x^2 + xy + y^2 = 13a$ y la recta $x + 2y = 3a$ en el caso de $a = 3$.

Nos interesan soluciones enteras. La recta $x+2y=3a$ siempre tendrá puntos enteros (recuerde la identidad de Bézout). Sin embargo, la elipse $x^2+xy+y^2=13a$ puede no tener ningún punto entero.

Si $a \equiv 2 \pmod 3$, entonces la ecuación $x^2+xy+y^2=13a$ nos da una congruencia

$$x^2+xy+y^2 \equiv -1 \pmod 3,$$

y esto es imposible. En particular, podemos concluir que para $a=2,5$ las elipses $x^2+xy+y^2=13a$ no tienen puntos enteros.

En general, hay una manera de contar el número de puntos enteros sobre la elipse $x^2+xy+y^2=n$ en términos de n. La respuesta es la siguiente:

> Consideremos la ecuación $x^2+xy+y^2=n$ para $n=p_1^{e_1}\cdots p_s^{e_s}$.
> Si para algún i se tiene $p_i \equiv 2 \pmod 3$ y e_i es impar, entonces la ecuación no tiene soluciones enteras.
> En el caso contrario, el número de soluciones enteras es
>
> $$6 \prod_{p_i \equiv 1 \ (3)} (e_i+1).$$

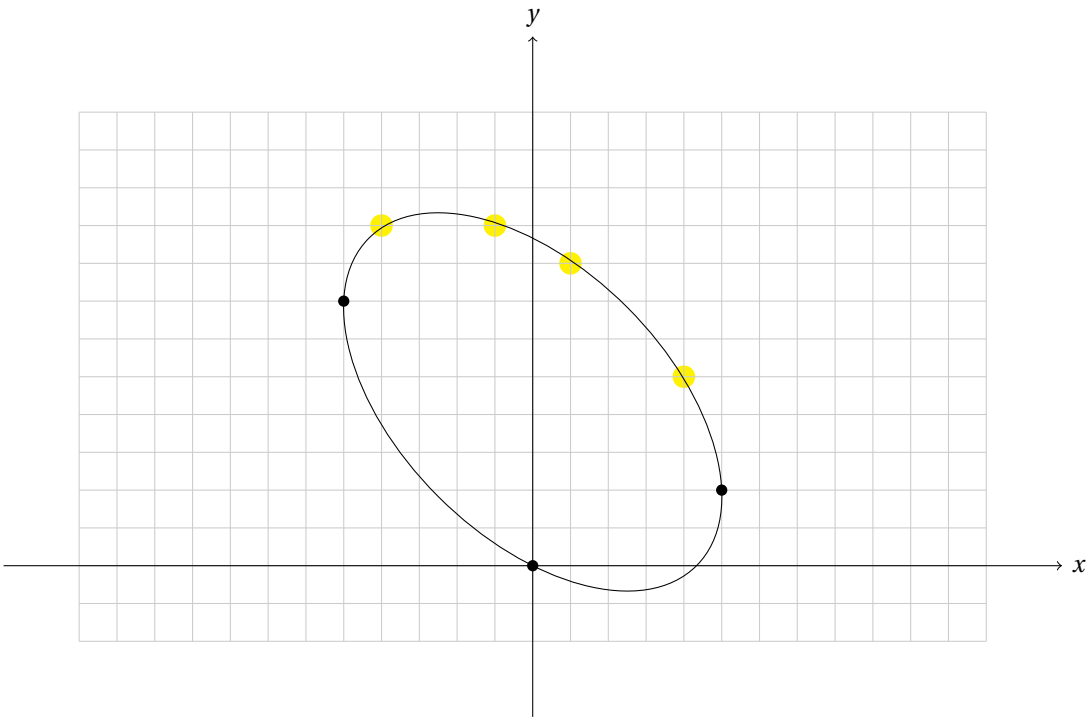
El número 6 sale por razones de simetría en las soluciones (note también que para $n=1$ hay 6 soluciones). En el dibujo de arriba se pueden observar 12 puntos enteros en el caso de $n=3\cdot 13$. La prueba del resultado de arriba es un poco complicada, pero me gustaría mencionarlo, como un bonito ejemplo de conteo aritmético. □

Otra opción. De una vez podemos analizar los puntos enteros en la elipse

$$3\,(x^2+xy+y^2) = 13\,(x+2y).$$

Siendo una figura acotada, la elipse tiene un número finito de puntos enteros, y en este caso se pueden ver las cotas $-5 \le x \le 5$, $0 \le y \le 9$, nada más considerando la ecuación como cuadrática en la variable x o y.

Si podemos hacer un buen dibujo, se ve que los puntos enteros son $(0,0)$ (este no nos interesa), $(-5,7)$, $(5,2)$. Pero los dibujos pueden ser engañosos. Por ejemplo, parece que $(4,5)$ es un punto en la elipse. Sustituyendo $(x,y)=(4,5)$, nos queda $3(x^2+xy+y^2)=183$ y $13(x+2y)=182$. Por esto $(4,5)$ es «casi» una solución.



La elipse $3(x^2+xy+y^2)=13(x+2y)$ con puntos enteros y puntos sospechosos

□

Problema 15 (IWYMIC 2019 Team contest)**.** Encontrar todos los posibles dígitos (a,b) (es decir, $0\le a,b\le 9$) tales que el número $2a1b9$ cumple la congruencia

$$2a1b9^{2019}\equiv 1 \pmod{13}.$$

Problema 16. Encontrar soluciones enteras $x,y>0$ de la ecuación

$$\frac{1}{\sqrt{x}}+\frac{1}{\sqrt{y}}=\frac{1}{\sqrt{20}}.$$

Solución. Podemos expresar

$$x=\frac{20y}{20+y-2\sqrt{20y}},$$

de donde necesariamente $\sqrt{20y}\in\mathbb{Z}$; es decir, $20y$ es un cuadrado. De manera completamente simétrica, $20x$ es un cuadrado. Pero esto implica que $x=5a^2$ e $y=5b^2$ para algunos $a,b\in\mathbb{Z}$. Sustituyendo en la ecuación $x=5a^2$ e $y=5b^2$, nos queda

$$\frac{1}{a}+\frac{1}{b}=\frac{1}{2}.$$

Aquí el resultado general es el siguiente.

Para ver cuáles son las soluciones enteras $u, v \in \mathbb{Z}$ de

$$\frac{1}{u} + \frac{1}{v} = \frac{1}{n},$$

se puede notar (¡ejercicio!) que esta ecuación es equivalente a

$$(u-n)(v-n) = n^2,$$

y por lo tanto las soluciones corresponden a los divisores de n^2

En nuestro caso particular $n = 2$, así que tenemos

$$(a-2)(b-2) = 4,$$

de donde

$$(a,b) = (3,6),\ (4,4),\ (6,3).$$

Podemos concluir que

$$(x,y) = (5a^2, 5b^2) = (45,180),\ (80,80)\ (180,45).$$

* * *

Algunas preguntas similares:

— ¿cuáles son las soluciones enteras $x, y > 0$ de $\frac{1}{\sqrt{x}} + \frac{1}{\sqrt{y}} = \frac{1}{\sqrt{n}}$ para $n = 63$?

— ¿cuántas soluciones enteras tiene la ecuación $\frac{1}{x} + \frac{1}{y} = \frac{1}{n}$ para $n = 2021$?

— Para $n = 1, 2, 3, \ldots$ fijo, sea $s(n)$ el número de soluciones enteras $x, y > 0$ de $\frac{1}{x} + \frac{1}{y} = \frac{1}{n}$.
Demuestre que $s(n)$ es impar.

— Demuestre que si $\text{mcd}(m,n) = 1$, entonces $s(mn) = s(m)\, s(n)$.
(En este caso se dice que $s(n)$ es una **función multiplicativa**.)

□