Algunas aplicaciones a primalidad (pruebas de irracionalidad):

Comencemos con algunas aplicaciones del resultado anterior para el caso en el que se tienen números primos involucrados.

<u>Corolario</u>: Las siguientes condiciones son equivalentes para todo $p \in \mathbb{N}$ con $p \geq 2$.

(a) p es primo.

(b) $\forall a, b \in \mathbb{Z}$, $p \mid ab \Rightarrow p \mid a$ o $p \mid b$.

• <u>Demostración</u>:

$(a) \Rightarrow (b)$: Supongamos que p es primo, y sean a y b en $\mathbb{Z}$ tales que $p \mid ab$.

- Si $p \mid a$, no queda nada que probar.
- Supongamos entonces que $p \nmid a$. Como p es primo, se tiene que $m.c.d.(a, p) = 1$. Luego, por el Lema de Euclides, como $p \mid ab$ y $m.c.d.(a, p) = 1$ concluimos que $p \mid b$.

(b) $\Rightarrow$ (a): Supongamos que se cumple la siguiente implicación para todo $a, b \in \mathbb{Z}$.

$$p \mid ab \Longrightarrow p \mid a \text{ o } p \mid b. \quad (*)$$

Una manera de demostrar que p es primo es probando que sus únicos divisores positivos son 1 y p.

Sea entonces $a \in \mathbb{Z}^+$ un divisor de p. Tenemos que existe $b \in \mathbb{Z}^+$ tal que $p = ab$. Luego, $p \mid ab$.

Usando $(*)$, nos queda que $p \mid a$ o $p \mid b$.

- Si $p \mid a$, entonces $a = p$ ya que $a \mid p$ y $a, p \in \mathbb{Z}^+$.
- Si $p \nmid a$, entonces $p \mid b$. Luego, existe $q \in \mathbb{Z}^+$ tal que $b = qp$.

Así, $p = ab = aqp$, es decir,

$$0 = p(aq - 1)$$

Como $p \geqslant 2$, debe ocurrir que $aq = 1$.

$a, q \in \mathbb{Z}^+$ y $aq = 1 \Longrightarrow a = q = 1.$

Por lo tanto, 1 y p son los únicos divisores positivos de p, es decir, p es primo. ■

<u>Corolario</u>: Si p es primo, entonces $\sqrt{p}$ es irracional.

- <u>Demostración</u>: Supongamos que $\sqrt{p}$ es racional. Luego, $\sqrt{p} = \frac{a}{b}$ donde $a, b \in \mathbb{Z}^+$ con $m.c.d.(a, b) = 1$.

Tenemos así que $a = b\sqrt{p}$. Luego,

$$a^2 = p \cdot b \cdot b.$$

de donde $a \mid p \cdot b \cdot b$. Como $m.c.d.(a, b) = 1$, por el lema de Euclides tenemos que $a \mid pb$. Aplicando de nuevo el mismo resultado, nos queda que $a \mid p$. Al ser p primo, tenemos que $a = 1$ o $a = p$.

- Si $a = 1$, entonces $1 = p \cdot b^2$. Como $p, b^2 \in \mathbb{Z}^+$, tenemos que $p = 1$, lo cual es una contradicción.
- Si $a = p$, entonces $p^2 = p\,b^2$. Luego,

$$0 = p(p - b^2).$$ Como $p \geq 2$, nos queda

$$p = b^2 = b \cdot b$$

Se tiene así que $b \mid p$, por lo cual $b=1$ o $b=p$.

Si $b=1$, tenemos $p = 1^2 = 1$, lo cual es una contradicción

Si $b=p$, tenemos $p = p^2$, es decir,

$$0 = p(1-p),$$

de donde, $p=0$ o $p=1$. En cualquiera de los casos se tiene una contradicción.

Por lo tanto, $\sqrt{p}$ es irracional. ■

Obs: • Si p es compuesto, no se puede concluir sobre la racionalidad de $\sqrt{p}$. Por ejemplo, 4 y 6 son compuestos, y además $\sqrt{4}$ es racional y $\sqrt{6}$ irracional.

• Si $\sqrt{p}$ es racional, entonces p es compuesto.

Veamos ahora otro criterio para probar que un número dado es primo.

Proposición: Sea $a \in \mathbb{Z}^+$ con $a > 1$.
Si a es compuesto, entonces a tiene un divisor primo p tal que $p \leq \sqrt{a}$.

Observación: El contrarrecíproco del resultado anterior nos da un criterio para probar que un número dado es primo:

Si $p_1, \dots, p_m$ son los primos menores o iguales que $\sqrt{a}$ y a no es múltiplo de ninguno de ellos, entonces a es primo

$$\left(\begin{array}{l} 2 \leq p_1 < \cdots < p_m \leq \sqrt{a} \\ p_i \text{ primo } \forall i \in \{1, \dots, m\} \\ p_i \nmid a \ \ \forall i \in \{1, \dots, m\} \end{array} \Longrightarrow a \text{ es primo} \right)$$

Ejemplo: 101 es primo. En efecto, $\sqrt{101} \approx 10.05$
2, 3, 5 y 7 son los primos menores o iguales que $\sqrt{101}$. Como 101 no es múltiplo de ninguno de ellos, entonces 101 es primo.

• **Demostración de la proposición:**

Sea $a \in \mathbb{Z}^+$ con $a > 1$ compuesto.

• Veamos primero que a posee un divisor primo.

Al ser a compuesto, existen $1 < b, c < a$ tales que $a = bc$. Si b o c es primo, no queda nada que demostrar. En caso contrario (b y c compuestos), repetimos el argumento anterior hasta encontrar un divisor primo.

• Por la parte anterior, $a = pc$ con p primo y

$$1 \leq p \leq c.$$

Multiplicamos la desigualdad anterior por p.

$$p \leq p^2 \leq pc = a.$$

Es decir, $p^2 \leq a$. Es decir, $p \leq \sqrt{a}$. ∎

Mínimo común múltiplo

Así como estudiamos el conjunto de divisores comunes de un par de enteros, podemos hacer lo mismo con su conjunto de múltiplos comunes.

<u>Definición</u>: Dados $a, b \in \mathbb{Z}$, diremos que $c \in \mathbb{Z}$ es un <u>múltiplo común de a y b</u> si

$$a \mid c \quad y \quad b \mid c.$$

Denotaremos por $Mul^+(a,b)$ al conjunto de múltiplos comunes positivos de a y b, para el caso en el cual $a \neq 0$ y $b \neq 0$.

<u>Observación</u>: ① Si c es un múltiplo común de a y b, con $a=0$ o $b=0$, entonces $c=0$. Por tal razón, no es interesante estudiar el conjunto de múltiplos comunes de a y b cuando $a=0$ o $b=0$.

② $Mul^+(a,b) \neq \emptyset$ ya que $|ab| \in Mul^+(a,b)$.

Además, $Mul^+(a,b)$ es un subconjunto de $\mathbb{Z}$ acotado inferiormente. Esto da lugar a la siguiente definición.

<u>Definición</u>: Dados $a, b \in \mathbb{Z}$ con $a \neq 0$ y $b \neq 0$, el mínimo común múltiplo de a y b, denotado por $m.c.m.(a,b)$, se define como el elemento mínimo de $Mul^+(a,b)$.

En otras palabras, m.c.m.(a,b) es el menor entero positivo que es múltiplo común de a y b.

- Si $a=0$ o $b=0$, entonces m.c.m.$(a,b)=0$.

Caracterizamos el concepto anterior en el siguiente resultado:

<u>Proposición</u>: Sean $a,b \in \mathbb{Z}$ no nulos. Entonces $m = $ m.c.m.(a,b) si y solamente si $m \mid c$ para todo $c \in Mul^{+}(a,b)$, donde $m \in Mul^{+}(a,b)$.

- <u>Demostración</u>:

Supongamos primero que $m = $ m.c.m.(a,b), y sea $c \in Mul^{+}(a,b)$. Veamos que $m \mid c$.

Por el Teorema de la División Entera, tenemos que existen $q, r \in \mathbb{Z}$ tales que

$$c = q \cdot m + r \quad \text{con} \quad 0 \leq r < m.$$

$$r = c - q \cdot m.$$

Como $a \mid c$ y $a \mid b$, $c = xa$ y $c = yb$ para algunos $x, y \in \mathbb{Z}$. De manera similar,

$$c = x'a \quad y \quad c = y'b$$

para algunos $x', y' \in \mathbb{Z}$.

Luego,

$$r = c - qm = xa - qx'a = (x - qx')a$$

y

$$r = c - qm = yb - qy'b = (y - qy')b$$

Entonces, r es un múltiplo común de a y b.
Como m es el menor entero positivo que es múltiplo común de a y b, se tiene que $r = 0$ (ya que $0 \leq r < m$).
Por lo tanto, $c = qm$, es decir, $m \mid c$.

Ahora supongamos que $m \mid c$ para todo $c \in Mul^+(a,b)$.
En particular, $m \mid m.c.m.(a,b)$, por lo cual

$$m \leq m.c.m.(a,b).$$

Como $m.c.m.(a,b) = \min Mul^+(a,b)$ y $m \in Mul^+(a,b)$, se concluye que

$$m = m.c.m.(a,b). \blacksquare$$

No hace falta desarrollar un método para calcular $m.c.m.(a,b)$, debido a la siguiente relación con el $m.c.d.(a,b)$.

Teorema: Sean $a, b \in \mathbb{Z}$ no nulos. Entonces,

$$m.c.d.(a,b) \cdot m.c.m.(a,b) = |ab|.$$

• **Demostración:** Se puede asumir que $a, b > 0$. En efecto, ya sabemos que $mcd(a,b) = mcd(|a|, |b|)$. Se puede notar lo mismo con el concepto de mínimo común múltiplo, es decir,

$$mcm(a,b) = mcm(|a|, |b|).$$

Sea $d = mcd(a,b)$. Note que $\frac{ab}{d} \in \mathbb{Z}^+$ ya que $d|a$ y $d|b$. Denotamos

$$m := \frac{ab}{d}.$$

Veamos que $mcm(a,b) = m$.

$mcm(a,b) = m$ si y sólo si $m \in Mul^+(a,b)$ y $m|c$ para todo $c \in Mul^+(a,b)$.

① $m \in Mul^+(a,b)$:

- $m = \frac{ab}{d} = a \cdot \frac{b}{d}$ donde $\frac{b}{d} \in \mathbb{Z}^+$ (m es múltiplo de a)
- $m = \frac{ab}{d} = b \cdot \frac{a}{d}$ donde $\frac{a}{d} \in \mathbb{Z}^+$ (m es múltiplo de b)

$\therefore$ $m \in Mul^+(a,b)$.

② Ahora, sea $c \in Mult^+(a,b)$. Veamos que $m \mid c$.
Como $c \in Mult^+(a,b)$, tenemos que existen $p, q \in \mathbb{Z}$ tales que

$$c = ap \quad y \quad c = bq.$$

Denotemos $a^* = \dfrac{a}{d}$ y $b^* = \dfrac{b}{d}$ (cofactores).

Veamos que $b^* \mid p$.

$$ap = bq \Rightarrow da^*p = db^*q$$
$$d(a^*p - b^*q) = 0.$$

$$d \neq 0 \Rightarrow a^*p = qb^*.$$

Como $mcd(a^*, b^*) = 1$, y además $b^* \mid a^*p$, por el Lema de Euclides se tiene que $b^* \mid p$.
Luego, existe $k \in \mathbb{Z}$ tal que $p = kb^*$.
Entonces,

$$c = ap = akb^* = k\frac{ab}{d} = km,$$

es decir, $m \mid c$.

Por lo tanto, $m = mcm(a,b)$. ■

Corolario: Sean $a, b \in \mathbb{Z}$ no nulos. Entonces, a y b son primos relativos si y solamente si

$$m.c.m.(a,b) = |ab|.$$

Damos a continuación algunas propiedades adicionales del mínimo común múltiplo.

Proposición (propiedades del mínimo común múltiplo): Sean $a, b \in \mathbb{Z}$ no nulos. Las siguientes propiedades se cumplen:

① $m.c.m.(a,b) = m.c.m.(|a|,|b|)$

② $m.c.m.(ca, cb) = |c|\, m.c.m.(a,b) \quad \forall c \in \mathbb{Z}$.

③ Si $c \neq 0$, $c|a$ y $c|b$, entonces

$$m.c.m.\left(\frac{a}{c}, \frac{b}{c}\right) = \frac{m.c.m.(a,b)}{|c|}.$$

· Demostración:

① Es inmediato de la definición de mínimo común múltiplo.

② Si $c = 0$ entonces

$$mcm(0\cdot a, 0\cdot b) = mcm(0,0) = 0 = 0 \cdot mcm(a,b).$$

Podemos asumir $c \neq 0$.

Por el teorema anterior, tenemos

$$\text{mcm}(ca, cb) = \frac{|ca \cdot cb|}{\text{mcd}(ca, cb)} = \frac{|c|^2 \, |ab|}{|c| \, \text{mcd}(a,b)}$$

$$= |c| \cdot \frac{|ab|}{\text{mcd}(a,b)} = |c| \cdot \text{mcm}(a,b).$$

③ Por la parte anterior, tenemos

$$|c| \cdot \text{mcm}\left(\frac{a}{c}, \frac{b}{c}\right) = \text{mcm}\left(c \cdot \frac{a}{c}, c \cdot \frac{b}{c}\right) = \text{mcm}(a,b)$$

Como $c \neq 0$, nos queda

$$\text{mcm}\left(\frac{a}{c}, \frac{b}{c}\right) = \frac{\text{mcm}(a,b)}{|c|}. \quad \blacksquare$$

Cerramos con un ejemplo.

Ejemplo:

Hallar $\text{mcm}(12, 8)$.

$12 = 2^2 \cdot 3$ y $8 = 2^3$.

Luego, $\text{mcm}(12, 8) = 24$.

O también, $\text{mcd}(12, 8) = 4$, por lo cual

$$\text{mcm}(12, 8) = \frac{12 \cdot 8}{\text{mcd}(12, 8)} = \frac{12 \cdot 8}{4} = 3 \cdot 8 = 24.$$

Ecuaciones diofánticas

Supongamos que tenemos $a, b \in \mathbb{Z}$ y $n \in \mathbb{N}$ fijos, y nos piden hallar el conjunto de pares de números (x, y) tales que

$$ax + by = n. \quad (*)$$

En otras palabras,

¿cuáles son las soluciones (x, y) de la ecuación anterior?

¿existen soluciones en primer lugar?

Las respuestas a estas interrogantes dependen de en dónde vamos a buscar las soluciones (x, y). Por ejemplo, si buscamos x e y en $\mathbb{R}$, entonces el conjunto de soluciones (x, y) corresponde a la recta de ecuación $(*)$.

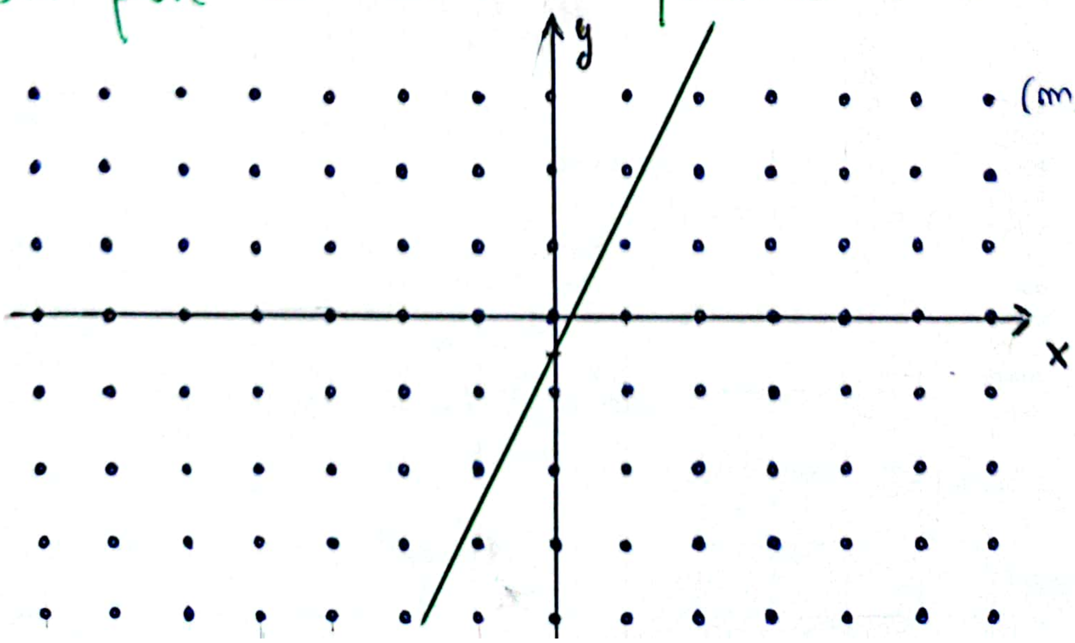
Ahora, si queremos buscar x e y en $\mathbb{Z}$, las respuestas a las preguntas anteriores pueden no ser tan inmediatas. Puede ocurrir inclusive que $(*)$ no tenga soluciones enteras.

Ejemplo: La ecuación $4x-2y=1$ no tiene solución en $\mathbb{Z}\times\mathbb{Z}$. Existen varias maneras de notar esto:

a) Si existen x e y en $\mathbb{Z}$ tales que $1=4x-2y$ entonces $1=2(2x-y)$, es decir, estaríamos diciendo que 1 es par, lo cual es absurdo.

b) Si existen x e y en $\mathbb{Z}$ tales que $1=4x-2y$ entonces por un resultado previo tenemos que 4 y -2 son primos relativos, lo cual es absurdo ya que $\operatorname{mcd}(4,-2)=2$.

c) La recta $4x-2y=1$ (es decir, $y=2x-\frac{1}{2}$) no pasa por la nube de puntos $(m,n)\in\mathbb{Z}\times\mathbb{Z}$.



Las ecuaciones de la forma

$$ax + by = n$$

con $a, b, n \in \mathbb{Z}$ se conocen como <u>ecuaciones diofánticas lineales</u>, y deben su nombre al matemático griego Diofanto de Alejandría (siglo III o IV D.C.). Si bien Diofanto no es quien descubre este tipo de ecuaciones, sí hizo un trabajo relevante en cuanto a la organización de los conocimientos existentes en torno a este tipo de ecuaciones.

Nuestro estudio de las ecuaciones diofánticas lineales se centrará en hallar condiciones necesarias y suficientes para que $ax + by = n$ tenga solución (en $\mathbb{Z} \times \mathbb{Z}$). Posteriormente, una vez conozcamos al menos una solución de $ax + by = n$ (en caso de existir), veremos cómo describir todas las soluciones.

Del ejemplo anterior, podemos intuir que el $mcd(a, b)$ tiene algo que decir respecto a la existencia de soluciones de $ax + by = n$. En efecto, tal es el caso, y lo explica detalladamente el siguiente resultado.

Teorema (existencia de soluciones de ecuaciones diofánticas lineales): Sean $a, b, n \in \mathbb{Z}$ y $d := mcd(a,b)$. Entonces $ax + by = n$ tiene solución $x, y \in \mathbb{Z}$ si y solamente si $d \mid n$.

• **Demostración:** Supongamos primero que $ax+by=n$ tiene solución, digamos $(x_0, y_0) \in \mathbb{Z} \times \mathbb{Z}$.

$$(ax_0 + by_0 = n)$$

Como $d = mcd(a,b)$, tenemos que $d \mid a$ y $d \mid b$. Luego $d \mid (ax_0 + by_0)$, es decir, $d \mid n$.

Ahora supongamos que $d \mid n$. Por el Teorema de Bézout, existen $x_1, y_1 \in \mathbb{Z}$ tales que

$$ax_1 + by_1 = d. \quad (*)$$

Por otro lado, como $d \mid n$, existe $q \in \mathbb{Z}$ tal que

$$n = qd.$$

Multiplicamos $(*)$ por q, y obtenemos

$$a(qx_1) + b(qy_1) = qd = n.$$

Por lo tanto, $x_0 = qx_1$ e $y_0 = qy_1$ es solución en $\mathbb{Z} \times \mathbb{Z}$ de la ecuación $ax + by = n$. ∎

Las ecuaciones diofánticas lineales pueden aparecer a la hora de querer resolver ciertos problemas cotidianos, como veremos a continuación.

<u>Ejemplo</u>: Link cuenta con 563 Rupias para comprar bananas y manzanas. El precio de cada banana es de 13 Rupias, y el de cada manzana es de 7 Rupias. Asumiendo que link quiere gastar todo el dinero, determine (en caso de ser posible) cuántas bananas y cuántas manzanas puede comprar.

Sean B = cantidad de bananas, y
M = cantidad de manzanas.

Se quiere saber si existen $B, M \in \mathbb{Z}^+$ tales que

$$13B + 7M = 563.$$

Como $mcd(13, 7) = 1$ y claramente $1 \mid 563$, por el teorema anterior sabemos que existen B_0 y M_0 (en $\mathbb{Z}$, no necesariamente en $\mathbb{Z}^+$) tales que

$$13B_0 + 7M_0 = 563.$$

Em efecto, podemos notar que

$$13(-1) + 7 \cdot 2 = 1,$$

de donde

$$13(-563) + 7 \cdot 1126 = 563.$$

Entonces, si bien $B_0 = -563$ y $M_0 = 1126$ es una solución de $13B + 7M = 563$, no es una solución al problema planteado, ya que no es posible comprar una cantidad negativa de bananas.

¿Puede entonces Link resolver su problema?

Para ayudar a Link, necesitamos un poco más de teoría. Concretamente, conviene conocer el conjunto de todas las soluciones de la ecuación $13B + 7M = 563$.

Conociendo al menos una solución de una ecuación diofántica $ax + by = n$, es posible determinar el resto.

Teorema (descripción del conjunto solución de una ecuación diofántica): Sean $a, b, n \in \mathbb{Z}$ no nulos tales que $d := mcd(a,b) \mid n$. Si $(x_0, y_0) \in \mathbb{Z} \times \mathbb{Z}$ es una solución de la ecuación diofántica lineal

$$ax + by = n,$$

entonces cualquier otra solución $(x,y) \in \mathbb{Z} \times \mathbb{Z}$ es de la forma

$$x = x_0 + k \cdot \frac{b}{d} \quad \text{e} \quad y = y_0 - k \cdot \frac{a}{d}, \quad \text{con } k \in \mathbb{Z}.$$

· Demostración: Sean (x_1, y_1) y (x_0, y_0) soluciones de $ax + by = n$. Luego,

$$ax_1 + by_1 = n = ax_0 + by_0$$

$$a(x_1 - x_0) = b(y_0 - y_1)$$

$$\frac{a}{d}(x_1 - x_0) = \frac{b}{d}(y_0 - y_1).$$

Tenemos entonces que $\frac{a}{d} \mid \frac{b}{d}(y_0 - y_1)$. Como $mcd\left(\frac{a}{d}, \frac{b}{d}\right) =$

por el Lema de Euclides se obtiene

$$\frac{a}{d} \mid (y_0 - y_1).$$

Luego, existe $k \in \mathbb{Z}$ tal que $y_0 - y_1 = k \cdot \frac{a}{d}$, por lo cual

$$y_1 = y_0 - k \cdot \frac{a}{d}.$$

Así, $\frac{a}{d}(x_1 - x_0) = \frac{b}{d} \cdot k \cdot \frac{a}{d}$

$$\frac{a}{d}\left(x_1 - x_0 - k\frac{b}{d}\right) = 0.$$

Como $a/d \neq 0$, nos queda $x_1 = x_0 + k \cdot \frac{b}{d}$. $\blacksquare$

Ejemplo: Volviendo a Hyrule, la ecuación

$$13B + 7M = 563$$

tiene por solución $B_0 = -563$ y $M_0 = 1126$. Entonces, todas las soluciones son de la forma

$$B = B_0 + k7 \quad \text{y} \quad M = M_0 - k \cdot 13.$$
$$B = 7k - 563 \qquad M = 1126 - 13k.$$

El problema se reduce a buscar los valores de k para los cuales $B > 0$ y $M > 0$. Lo primero a notar es que $k > 0$. Más aún, $k = 81$ es el menor entero positivo tal que

$$B = 7 \cdot 81 - 563 = 567 - 563 = 4.$$

Además, $M = 1126 - 13 \cdot 81 = 73.$

Por otro lado,

- $K = 82$: $B = 7 \cdot 82 - 563 = 11$

  $M = 1126 - 13 \cdot 82 = 60$

- $K = 83$: $B = 7 \cdot 83 - 563 = 18$

  $M = 1126 - 13 \cdot 83 = 47$

- $K = 84$: $B = 7 \cdot 84 - 563 = 25$

  $M = 1126 - 13 \cdot 84 = 34$

- $K = 85$: $B = 7 \cdot 85 - 563 = 32$

  $M = 1126 - 13 \cdot 85 = 21$

- $K = 86$: $B = 7 \cdot 86 - 563 = 39$

  $M = 1126 - 13 \cdot 86 = 8$.

Para $K \geq 87$, ocurre que $M < 0$.

Por lo tanto, Link puede comprar bananas y manzanas, gastando todo el dinero, dentro de las siguientes selecciones de cantidades (B, M):

$(4, 73)$, $(11, 60)$, $(18, 47)$, $(25, 34)$, $(32, 21)$

o $(39, 8)$.

En varios problemas cuya solución involucra plantean y resolver una ecuación diofántica, interesa hallar soluciones positivas. Hay algunas herramientas que permiten darnos cuenta de cuándo esto es posible. Mencionamos algunos a continuación.

Proposición: Sean $a, b \in \mathbb{Z}^+$ primos relativos.

① Si $a, b > 1$ entonces no existen $x, y \in \mathbb{N}$ tales que
$$ax + by = ab - a - b.$$

② Si $n \geq ab - a - b + 1$, entonces existen $x, y \in \mathbb{N}$ tales que
$$ax + by = n.$$