# Primer Entrenamiento de Teoría de Números

**Jesús Liceaga**
jose.liceaga@cimat.mx
28 de agosto de 2021

---

El objetivo del presente documento es dar una introducción a la Teoría de Números, enfocándonos a la resolución de problemas. Comenzaremos introduciendo los conceptos de divisibilidad y números primos, para luego enunciar el Teorema Fundamental de la Aritmética. Posteriormente, hablaremos sobre el algoritmo de la división, el mínimo común múltiplo, el máximo común divisor y las combinaciones lineales. Si tienes alguna duda, siéntete en confianza de preguntarle al entrenador que tengas delante o de mandarme un correo, que se encuentra debajo del título.

- Liceaga

## 1. Divisibilidad

Desde que estamos en primaria, nos enseñan cómo dividir un número entre otro. Si estos son enteros, hay veces en las que la división da otro número entero: por ejemplo, cuando dividimos 48 entre 8 obtenemos 6. Esto es tan importante que nos motiva a definir lo siguiente:

**Definición.** Decimos que un entero $a$ distinto de 0 divide a otro entero $b$ si existe un entero $k$ tal que $ak = b$, y en este caso escribimos $a|b$. Si $a$ no divide a $b$, escribimos $a \nmid b$.

La relación "$a$ divide a $b$" cumple algunas propiedades interesantes, que mencionamos a continuación. Es importante hacer notar que cuando trabajamos con enteros positivos a los resultados de la siguiente Proposición se le pueden quitar los valores absolutos.

**Proposición 1.** Sean $a, b, c, r, s$ números enteros.

1. Si $a|b$ y $b \neq 0$, entonces $|a| \leq |b|$.
2. Si $a|b$ y $b|c$ entonces $a|c$.
3. Si $a|b$ y $b|a$ entonces $|a| = |b|$.
4. Si $a|b$ y $a|c$ entonces $a|rb + sc$ para cualesquiera enteros $r$ y $s$.

**Demostración.**

1. Como $a|b$ y $b \neq 0$, entonces existe un entero $k \neq 0$ tal que $ak = b$, de donde $0 \leq |a||k| = |b|$. Puesto que $|k| \geq 1$, entonces $\frac{1}{|k|} \leq 1$, así que al multiplicar esta desigualdad por la igualdad anterior obtenemos que $|a| \leq |b|$.
2. Puesto que $a|b$ y $b|c$, existen enteros $k, m$ tales que $b = ak$ y $c = bm$, de donde $c = akm$, y como $km$ es un entero, concluimos que $a|c$.
3. Puesto que $a|b$, por 1) obtenemos que $|a| \leq |b|$, pero como también se tiene que $b|a$ entonces $|b| \leq |a|$, de donde $|a| = |b|$.
4. Puesto que $a|b$ y $a|c$, existen enteros $k, m$ tales que $b = ak$ y $c = am$. Así, $rb + sc = rak + sam = a(rk + sm)$, y como $(rk + sm)$ es un entero, concluimos que $a|rb + sc$.

Para ver cómo usar la Proposición anterior presentamos el siguiente ejemplo.

**Ejemplo.** Encuentra todos los enteros $n$ para los cuales $n|3n+4$.

**Solución.** Supongamos que $n|3n+4$. Como $n|3n$, por el punto 4 del Teorema anterior tenemos que

$$n|1\cdot(3n+4)+(-1)\cdot(3n)\Rightarrow n|4.$$

Por lo tanto, los únicos valores posibles son $n=\pm1,\pm2,\pm4$, y sustituyendo estos en la expresión original es fácil ver que en efecto la satisfacen.

Otro de los usos comunes del concepto de divisibilidad es el ver si un número es divisible entre otro en particular, para lo cual existen ciertos criterios que facilitan las cosas, algunos de los cuales son los siguientes:

- **Criterio del 2**: Un número es divisible entre 2 si su último dígito es divisible entre 2 (es decir, que sea par). *Ejemplo*: 234 es divisible entre 2 porque 4 es divisible entre 2.
- **Criterio del 3**: Un número es divisible entre 3 si la suma de sus dígitos es divisible entre 3. *Ejemplo*: 234 es divisible entre 2 porque sus dígitos suman 9.
- **Criterio del 4**: Un número es divisible entre 4 si el número formado por sus últimos 2 dígitos es divisible entre 4. *Ejemplo*: 1216 es divisible entre 4 porque 16 es divisible entre 4.
- **Criterio del 5**: Un número es divisible entre 5 si su último dígito es 0 o 5. *Ejemplo*: 255 es divisible entre 2 porque su último dígito es 5.
- **Criterio del 6**: Que cumpla los criterios del 2 y del 3. *Ejemplo*: 234 es divisible entre 6 porque ya vimos que satisface los criterios del 2 y del 3.
- **Criterio del 8**: Un número es divisible entre 8 si el número formado por sus últimos 3 dígitos es divisible entre 8. *Ejemplo*: 2008 es divisible entre 8 porque 8 es divisible entre 8.
- **Criterio del 9**: Un número es divisible entre 9 si la suma de sus dígitos es divisible entre 9. *Ejemplo*: 234 es divisible entre 2 porque sus dígitos suman 9.
- **Criterio del 11**: Un número es divisible entre 11 si la suma de sus dígitos en posiciones impares menos la suma de sus dígitos en posiciones pares es 11 o 0. *Ejemplo*: 9031 es divisible entre 11 porque (9 + 3) - (1 + 0) = 11.

Una vez vista toda esta teoría, es hora de hacer algunos problemas.

1. Para que un número de 7 cifras: $6a74b14$ sea múltiplo de 9 y de 11, ¿cómo deben ser $a$ y $b$?
2. Encuentra todos los enteros positivos $n$ tales que $n+2|2n+10$.
3. ¿Cuántos números menores a 1000 son múltiplos de 3 pero no de 5?
4. Encuentra todos los enteros positivos $a$ tales que $a^2|4a$.
5. Si $m$ y $n$ son enteros tales que $2m-n=3$, prueba que $m-2n$ es divisible entre 3.
6. Encuentra todos los enteros positivos $n$ tales que $3n+1|4n+9$
7. Encuentra el menor número a que cumple que $a+2a+3a+4a+5a+6a+7a+8a+9a$ es un número con todas sus cifras iguales.
8. Prueba que $a-b|a^n-b^n$ para $a$ y $b$ enteros.
9. Sean $a$ y $b$ enteros. Prueba que $17|2a+3b$ si y solo si $17|9a+5b$.

## 2. Números primos y el Teorema Fundamental de la Aritmética

Para esta sección nos concentraremos en un subconjunto de los enteros: los enteros positivos (aquellos mayores o iguales a 1). Entre estos números existen unos particularmente especiales: los números primos, pues son ïndivisiblesz nos permiten escribir a los demás enteros como productos de estos. En esta sección estudiaremos algunas propiedades de los números primos y terminaremos con uno de los resultados más fundamentales de la aritmética (que seguro ya se imaginan cómo se llamará). Pero, antes de comenzar, tenemos que hacernos algunas preguntas: ¿Qué son exactamente los números primos? ¿Y los compuestos?

**Definición.** Un entero positivo es un número primo si tiene exactamente 2 divisores positivos: 1 y él mismo. *Ejemplo:* 2 es primo, porque sus únicos divisores son 1 y 2.

**Definición.** Un entero positivo es un número compuesto si no es primo. Es decir, si tiene más de 2 divisores positivos. *Ejemplo:* 4 es compuesto, pues es divisible entre 1, 2 y 4.

Una vez que hemos definido bien estos conceptos, ahora sí podemos enunciar el Teorema Fundamental de la Aritmética. Su demostración es algo técnica y utiliza conceptos que veremos más adelante, por lo que la omitiremos.

**Teorema 1.** Todo entero positivo mayor que 1 es un número primo o bien se puede escribir de forma única salvo por el orden como producto de números primos.

En términos más intuitivos, lo que este teorema nos dice es que cualquier número se puede escribir como un primo por otro primo por otro primo (y así cuantas veces sea necesario, incluso con números iguales) y que ese número es el único que se puede escribir de esa forma particular. Por ejemplo, tenemos que $12 = 3 \cdot 2 \cdot 2$, como 3 y 2 son primos, este teorema nos dice que no podemos encontrar otra manera de escribir a 12 como producto de números primos, salvo si intercambiamos el orden de los factores en el producto anterior.
Finalmente, notemos que si tenemos un entero positivo $n$, lo escribimos como producto de primos y luego "juntamos" los primos poniendo exponentes, el Teorema Fundamental de la Aritmética nos dice que podemos escribir a $n$ de forma única como

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_n^{\alpha_n},$$

donde los $p_1, p_2, \dots, p_n$ son números primos distintos y los $\alpha_1, \alpha_2, \dots, \alpha_n$ enteros positivos.

## 3. El algoritmo de la división

Otra de las cosas que vimos en primaria, aprendimos y empezamos a hacer en automático sin pensarlas es el algoritmo de la división, en el cual colocábamos un entero (el dividendo) dentro de una "casita", otro afuera (el divisor) y hacíamos una serie de pasos para obtener otro entero (el cociente) y algo que sobraba (el residuo), que siempre era menor al número dentro de la casita. Pero, ¿Por qué pasa eso último? ¿Y cómo sabemos que ese residuo es único? El siguiente Teorema justifica esto, y será tu tarea probar una versión de este.

**Teorema 2.** Si $a, n$ son enteros, entonces existen enteros únicos $q$ y $r$ con $0 \leq r < |b|$ tales que

$$a = nq + r.$$

*Ejemplo:* Tomando $a = 12$ y $n = 5$, tenemos que $12 = 2 \cdot 5 + 2$.

Cuando en la expresión del Teorema anterior se da que $r = 0$, entonces es claro que $n|a$. De hecho, este tipo de expresiones son útiles cuando queremos ver si un número es divisible entre otro o para calcular residuos, pues si tomamos $a, b$ y $n$ enteros tales que $a = q_1 n + r_1$ y $b = q_2 n + r_2$, tenemos que

- $a+b=(q_1+q_2)m+(r_1+r_2)$.
- $a-b=(q_1-q_2)m+(r_1-r_2)$.
- $ab=q_1q_2n^2+r_1q_2n+r_2q_1n+r_1r_2=(q_1q_2n+r_1q_2+r_2q_1)n+r_1r_2$.

Así, si queremos encontrar el residuo que dejan $a+b$, $a-b$ y $ab$ al dividirlos entre $n$ basta ver el residuo que dejan $r_1+r_2$, $r_1-r_2$ y $r_1r_2$ al dividirlos entre $n$, respectivamente (¿Por qué?). Esta idea es muy potente, pues como verán en futuros entrenamientos, nos permitirá introducir el concepto de congruencia, que es muy útil en olimpiada. De momento, presentamos un ejemplo de su aplicación:

**Ejemplo.** ¿Qué residuo deja $10^{50}$ al dividirlo entre 3?
**Solución.** Para encontrar este residuo podríamos escribir un 1 seguido de cincuenta 0's y hacer la división, pero esto no suena muy conveniente. Entonces, intentemos usar lo que acabamos de ver. Como 10 deja residuo 1 al dividirlo entre 3, entonces $10\cdot 10=10^2$ deja residuo $1\cdot 1=1$ al dividirlo entre 3. Así, como $10^{50}$ equivale a multiplicar cincuenta 10's, al considerar los residuos estamos multiplicando cincuenta 1's, por lo que el residuo que dejará $10^{50}$ al dividirlo entre 3 será 1.

Ahora que has visto todo esto, toca hacer más problemas:

1. Encuentra todos los números primos entre 1 y 50.
2. El producto de tres enteros mayores que 1 y distintos entre sí es 100. ¿Cuáles son los tres enteros?
3. Prueba que si $p$ es un número primo mayor que 3 entonces $3|p^2-1$.
4. ¿Qué residuo queda al dividir $2^{2021}$ entre 3?
5. Prueba que si $a$ es un entero y $p$ un primo tal que $p|a^2$, entonces $p|a$.
6. Prueba que si $a$ y $n$ son enteros positivos, entonces existen enteros no negativos únicos $q$ y $r$ tales que $a=qn+r$. **Sugerencia:** para mostrar que existen, define a $q$ como el mayor entero tal que $qn\leq a<(q+1)n$ y encuentra a $r$. Para la parte de la unicidad supón que hay dos formas de hacerlo y llega a una contradicción.
7. Prueba que todo número primo mayor a 3 deja residuo 1 o 5 al dividirlo entre 6.
8. Prueba que ninguno de los números $1573, 157573, 15757573, \ldots$ es un número primo.

# 4. Mínimo común múltiplo y máximo común divisor

Dada una colección de enteros, a veces nos interesa estudiar al mayor entero que divide a todos o al menor entero (positivo) que sea divisible entre todos. Para esto, tenemos los conceptos de máximo común divisor y mínimo común múltiplo, que definimos a continuación.

**Definición.** Sea $n\geq 2$ un entero positivo y $a_1,\ldots,a_n$ $n$ enteros. Definimos al máximo común dívisor (MCD) de $a_1,\ldots,a_n$, denotado por $MCD(a_1,\ldots,a_n)$, como aquel entero $d$ tal que $d|a_1,\ldots,d|a_n$ y para cualquier $d'$ que divida a $a_1,\ldots,a_n$ se tiene que $d'\leq d$.

**Definición.** Sea $n\geq 2$ un entero positivo y $a_1,\ldots,a_n$ $n$ enteros. Definimos al mínimo común múltiplo (mcm) de $a_1,\ldots,a_n$, denotado por $mcm[a_1,\ldots,a_n]$, como aquel entero positivo $m$ tal que $a_1|m,\ldots,a_n|m$ y para cualquier $m'$ que sea divisible por $a_1,\ldots,a_n$ se tiene que $m'\geq m$.

Por ejemplo, tenemos que $MCD(8,4) = 4$ y que $mcm[3,40,8] = 120$. Seguramente ya sabes cómo calculamos estos números, pero siempre es bueno recordarlo, para lo cual enunciaremos la siguiente Proposición, cuya demostración se sigue de las definiciones y no escribiremos.

**Proposición 2.** Sean $a$ y $b$ enteros positivos tales que $a = p_1^{\alpha_1} \dots p_n^{\alpha_n}$ y $b = p_1^{\beta_1} \dots p_n^{\beta_n}$, con $\alpha_i, \beta_i \geq 0$ y $p_i$ un primo para $i = 1, \dots, n$. Entonces, se tiene que

$$MCD(a,b) = p_1^{\text{mín}(\alpha_1,\beta_1)} \dots p_n^{\text{mín}(\alpha_n,\beta_n)}$$
$$mcm[a,b] = p_1^{\text{máx}(\alpha_1,\beta_1)} \dots p_n^{\text{máx}(\alpha_n,\beta_n)}.$$

Es decir, para encontrar el máximo común divisor de $a$ y $b$ los descomponemos en factores primos y tomamos los factores comunes elevados a la menor potencia, mientras que para encontrar el mínimo común múltiplo multiplicamos todos los factores comunes y no comunes elevados a la mayor potencia.

A continuación, enunciaremos varias propiedades del MCD y el mcm.

**Proposición 3.** Sean $a, b$ números enteros distintos de 0. Entonces, se tiene que

1. $MCD(a,b) = MCD(|a|,|b|)$.
2. Si $a|b$, entonces $MCD(a,b) = |a|$.
3. $MCD(a,0) = |a|$.
4. Si $d = MCD(a,b)$ y definimos $a' = a/d$ y $b' = b/d$, tenemos que $MCD(a',b') = 1$.
5. Si $b = aq + r$ con $q$ y $r$ enteros, entonces $MCD(a,b) = MCD(a,r)$.
6. Se tiene que $MCD(a,b) \cdot mcm[a,b] = |ab|$.

**Demostración.** Solamente probaremos 5, para los demás puntos te dejaré el trabajo a ti.

Claramente, $MCD(a,b)|a$. Por otra parte, puesto que $r = b - aq$ y como también se tiene que $MCD(a,b)|b$, por el punto 4 de la Proposición 1 tenemos que $MCD(a,b)|r$. Así, por definición, $MCD(a,b) \leq MCD(a,r)$. De manera similar, $MCD(a,r)|a$ y, puesto que $MCD(a,r)|r$ y $b = aq + r$, nuevamente por el punto 4 de la Proposición 1 tenemos que $MCD(a,r)|b$, de donde por definición concluimos que $MCD(a,r) \leq MCD(a,b)$. Esta última desigualdad combinada con la mostrada anteriormente nos permite concluir que $MCD(a,b) = MCD(a,r)$, como queríamos demostrar.

Ahora, prepárate para los problemas (pero no temas):

1. Encuentra el máximo común divisor y el mínimo común múltiplo de 3600 y 780.
2. Prueba que para todo primo $p$, $\sqrt{p}$ no es un número racional.
3. Calcula $MCD(4655, 1309)$ usando únicamente los puntos 3 y 5 de la Proposición 3 (puedes usarlos varias veces).
4. Sean $a, b$ enteros tales que $MCD(a,b) = 1$. Prueba que $MCD(a+b, a-b) = 1$ o 2.
5. Se dice que una fracción $\frac{a}{b}$ es irreducible si $MCD(a,b) = 1$. Prueba que para todo entero positivo $n$ la fracción $\frac{21n+4}{14n+3}$ es irreducible.
6. Sean $m$ y $n$ enteros positivos con $m$ impar. Prueba que $MCD\left(2^m - 1, 2^n + 1\right) = 1$.
7. Determina todas las parejas $(a,b)$ de enteros positivos tales que el número
$$\frac{a^2(b-a)}{b+a}$$
es el cuadrado de un número primo.

## 5. Combinaciones lineales y algoritmo de Euclides

Para concluir este entrenamiento, hablaremos un poco de qué son las combinaciones lineales y cómo caracterizar al máximo común divisor con éstas.

**Definición.** Decimos que un entero $a$ es combinación lineal de los enteros $b$ y $c$ si existen enteros $x, y$ tales que

$$a = bx + cy.$$

Por ejemplo, 10 es combinación lineal de 3 y 2, pues $10 = 3 \cdot 2 + 2 \cdot 2$.
Una vez introducido este concepto, presentaremos el algoritmo de Euclides, que sirve para calcular el máximo común divisor de 2 números y que, si hiciste el problema 3 de la sección anterior, te resultará familiar.

**Teorema 3.** Dados los enteros positivos $a$ y $b$ , mediante la aplicación repetida del algoritmo de la división podemos obtener una sucesión de cocientes y residuos

$$\begin{aligned}
a &= bq_0 + r_0 && 0 \leq r_0 < b && (0)\\
b &= r_0 q_1 + r_1 && 0 \leq r_1 < r_0 && (1)\\
r_0 &= r_1 q_2 + r_2 && 0 \leq r_2 < r_1 && (2)\\
&\vdots\\
r_{n-2} &= r_{n-1} q_n + r_n && 0 \leq r_n < r_{n-1} && (n)\\
r_{n-1} &= r_n q_{n+1}, && && (n+1)
\end{aligned}$$

donde $r_n$ es el último residuo distinto de 0. Entonces, se tiene que $r_n$ es el máximo común divisor de $a$ y $b$.

Un par de comentarios sobre el algoritmo anterior, que a primera vista puede verse muy intimidante. En primer lugar, la prueba de que podemos llegar a un $r_n$ final y que es el máximo común divisor la omitiré, pues es algo dolorosa de escribir en computadora. Sin embargo, la idea es, como en el problema 3, usar los puntos 3 y 5 de la Proposición 3.
El otro es sobre algo que posiblemente te estés preguntando: "supongamos que entiendo lo que dice el Teorema 3, ¿Para qué lo quiero? Si se ve tedioso y ya sé otra manera de sacar el máximo común divisor de dos números?". Bueno, hay dos respuestas a esa pregunta: en primer lugar, como veremos después, tiene aplicaciones teóricas muy útiles, y en segundo lugar, es porque puede ser mucho más rápido que el otro cuando los números son muy grandes, pues factorizar es un trabajo más difícil de lo que parece. Si te gusta la computación, podrías investigar un poco más de esto.
Bueno, ahora sí, vamos a ver un ejemplo para intentar que quede más claro.

**Ejemplo.** Encuentre el máximo común divisor de 1309 y 728.
**Solución.** Apliquemos el proceso anterior, para lo cual sólo iremos usando el algoritmo de la división, tomando al dividendo de la ecuación $(i+1)$ igual al divisor de la ecuación $(i)$ y al divisor de la ecuación $(i+1)$ igual al residuo de la ecuación $(i)$:

$$\begin{aligned}
1309 &= 728 \cdot 1 + 581 && (0)\\
728 &= 581 \cdot 1 + 147 && (1)\\
581 &= 147 \cdot 3 + 140 && (2)\\
147 &= 140 \cdot 1 + 7 && (3)\\
140 &= 7 \cdot 20 + 0 && (4)
\end{aligned}$$

Como el último residuo no 0 fue 7, concluimos que $MCD(1309, 728) = 7$.

Utilizando el algoritmo de la división, podemos probar el siguiente Teorema:

**Teorema 4.** Sean $a$ y $b$ entero. Entonces, existen enteros $x, y$ tales que

$$MCD(a, b) = ax + by.$$

En efecto, si vamos despejando los residuos de abajo hacia arriba en el algoritmo de la división (empezando en la ecuación $(n)$) y sustituyendo llegaremos a una combinación lineal que funciona. Nuevamente, no probaremos este Teorema, sino que lo ilustraremos con el ejemplo anterior, escribiendo a 7 como combinación lineal de 1309 y 728.

**Ejemplo.** Escribe a 7 como combinación lineal de 1309 y 728.

**Solución.** Considerando la numeración del ejemplo anterior, al despejar 7 de la ecuación (3) obtenemos que

$$7 = 147 - 140 \cdot 1. \qquad (5)$$

Luego, despejando 140 de la ecuación (2) obtenemos que $140 = 581 - 147 \cdot 3$, y sustituyendo esto en la ecuación (5) que

$$7 = 147 - (581 - 147 \cdot 3) \cdot 1 = 147 \cdot 4 - 581 \cdot 1. \qquad (6)$$

Nuevamente, despejando 147 de (1) llegamos a que $147 = 728 - 581 \cdot 1$, y sustituyendo en (6) a que

$$7 = (728 - 581 \cdot 1) \cdot 4 - 581 \cdot 1 = 728 \cdot 4 - 581 \cdot 5. \qquad (7)$$

Finalmente, despejando 581 de (0) tenemos que $581 = 1309 - 728 \cdot 1$ y así, sustituyendo en (7), que

$$7 = 728 \cdot 4 - (1309 - 728 \cdot 1) \cdot 5 = 728 \cdot 9 - 1309 \cdot 5.$$

Es decir, $7 = 1309 \cdot (-5) + 728 \cdot (9)$.

Para terminar, veamos que el máximo común divisor de dos números y las combinaciones lineales de éstos se relacionan de una manera especial.

**Teorema 5.** Si $a$ y $b$ son enteros positivos y $d = ax + by$ es su combinación lineal positiva mínima, entonces $d = MCD(a, b)$.

**Demostración.** Para ver esto, probaremos que $d$ divide a $a$ y $b$ y que además es el máximo entre todos los divisores comunes. Por el Algoritmo de la División, se tiene que $a = dq + r$ con $0 \leq r < d$. Como $d = ax + by$, al sustituir obtenemos que $a = (ax + by)q + r$, de donde $r = a(1 - xq) + b(-yq)$. Dado que $r < d$ y $d$ es la combinación lineal positiva mínima de $a$ y $b$, no es posible que $r > 0$, de donde $r = 0$ y, por lo tanto, $d|a$. De manera análoga se muestra que $d|b$.

Como $d|a$ y $d|b$, entonces por definición $d \leq MCD(a, b)$. Por otra parte, como $MCD(a, b)|a$ y $MCD(a, b)|b$, se tiene que $MCD(a, b)|ax + by$, es decir, que $MCD(a, b)|d$, de donde $MCD(a, b) \leq d$. Así, gracias a las dos desigualdades anteriores, concluimos que $d = MCD(a, b)$.

Bueno, ahora sí, te toca hacer los últimos problemas del entrenamiento.

1. Encuentra el máximo común divisor de 2210 y 980 y escríbelo como combinación lineal de estos.
2. Sean $a, b$ y $d$ enteros positivos tales que $d|a$, $d|b$ y $d$ es combinación lineal de $a$ y $b$. Prueba que $d = MCD(a, b)$.
3. Si $a$ y $b$ son enteros tales que $MCD(a, b) = 1$, muestra que $MCD(a^2, b^2) = 1$.
4. Sean $a, b$ y $n$ enteros positivos. Prueba que $MCD(an, bn) = n \cdot MCD(a, b)$.
5. Prueba que si $a|bc$ y $MCD(a, b) = 1$ entonces $a|c$.
6. Sean $a$ y $b$ enteros tales que $MCD(a, b) = 1$. Demustra que $MCD(a + b, a^2 - ab + b^2) = 1$ o 3.