2. DIVISIBILIDAD

2. 1. *Divisibilidad: Características*

1.1 Propiedades de la divisibilidad.

Si a y b son dos enteros, $b \neq 0$, decimos que b *divide* a a si existe un entero c tal que $a = bc$. Cuando b divide a a decimos que b es factor de a y que a es múltiplo de b. La notación $b \mid a$ indica que b divide a a. Escribiremos $b \nmid a$ cuando b no divide a a.
Si a,b,c y $d \in \mathbb{Z}$ son enteros, entonces las propiedades de la divisibilidad de los números enteros podemos resumirlas en:

Si a es divisor de b también será divisor de cualquier múltiplo de b. Sean $s,t \in \mathbb{Z}$. Si $b = as$ y $d = bt$, será $d = a(st)$ por tanto, si $a \mid b$ también $a \mid b(st)$.

Si a es divisor de b y de c, también lo será de $b \pm c$, supuesto $b \geqq c$. Sean $s,t \in \mathbb{Z}$. Si $b = as$ y $c = ct$, sumando o restando miembro a miembro, obtendremos, $b \pm c = as \pm at = a(s \pm t)$ por tanto, si $a \mid b$ y $a \mid c$ también $a \mid a(s \pm t)$.

Si a es divisor de b y b lo es de c, entonces a será divisor de c. Para $s,t \in \mathbb{Z}$, puesto que si $b = as$ y $c = bt$, será $c = a(st)$ por tanto, si $a \mid b$ y $b \mid c$ entonces $a \mid c$.

Si a divide a la suma $b + c$ de dos enteros y a uno de los sumandos, por ejemplo, al b, también dividirá al otro c. Sean $s,t \in \mathbb{Z}$. Si $b + c = as$ y $b = at$, como $(b + c) - b = c = a(s - t)$, supuesto $s \geqq t$ entonces, si $a \mid (b + c)$ y $a \mid b$ también $c \mid a(s - t)$.

Si a divide a la diferencia $b - c$ de dos enteros y a uno de ellos, por ejemplo, al b, también dividirá al otro c. Sean $s,t \in \mathbb{Z}$. Si $b - c = as$ y $b = at$, como $b - (b - c) - b = c = a(t - s)$, supuesto $t \geqq s$ entonces, si $a \mid (b - c)$ y $a \mid b$ también $c \mid a(t - s)$.

Otras propiedades de la divisibilidad pueden ser que:

Si $u \mid 1$ con $u \in \mathbb{Z}$ entonces, u se denomina unidad.
Si $1 \mid n$ implica que cualquier n, $n \in \mathbb{Z}$ es divisible por la unidad.
Si $n \mid 0$ implica que $n = 0$ y por tanto, cada entero divide a cero.
Si $0 \mid n$ implica que $n \neq 0$ ya que el cero sólo divide al cero
Si $d \mid n$ entonces $n \mid d$ se llama el divisor conjugado de d.
Si $d \mid a$ y $d \mid c$ entonces $d \mid bc$ donde d es el común divisor de a y b.

1.2 Criterios de la divisibilidad.

Todos los números primos conocidos terminan en $1,3,7$ *ó* 9 aunque no todos los números que terminan en $1,3,7$ *ó* 9 son primos. Las terminaciones en $2,5$ *ó* 0 denotan números que son divisibles por $2,5$ *ó* 10 luego, las dudas en la factorización de un número las encontramos en aquéllos que terminan en $1,3,7$ *ó* 9, ya que pueden ser primos o compuestos.
Todo entero positivo N se puede escribir como $N = 10d + u$, dónde d y u representan, respectivamente, las decenas y unidades de N, con $0 \leqq u \leqq 9$.
Para determinar el criterio de divisibilidad de un número podemos utilizar sistemas modulares, de tal forma que $10d + u \equiv 0 (mód.N)$.

Empecemos por demostrar los criterios de divisibilidad de los números con terminación en 1, como el $11,21,31,41,51,61,71,81,91\ldots$
Un número es divisible por 11 si, y sólo si:

1. La suma de sus decenas más 10 veces sus unidades es 11 o múltiplo de 11.
2. La diferencia entre sus decenas y sus unidades es $0,11$ o múltiplo de 11.

Sea $10d+u\equiv 0(mód.11)$. Si multiplicamos la ecuación por 10 y sacamos restos, respecto al módulo 11, resulta $d+10u\equiv 0(mód.11)$ o bien $d\equiv u(mód.11)$, por lo que se demuestra que $11|N$ si, y sólo si $11|(d+10u)$ *ó* $11|(d-u)$.
Un número es divisible por 21 si, y sólo si:

1. La suma de sus decenas más 19 veces sus unidades es 21 o múltiplo de 21.
2. La diferencia entre sus decenas y 2 veces sus unidades es 0, 21 o múltiplo de 21.

Sea $10d+u\equiv 0(mód.21)$. Si multiplicamos la ecuación por 19 y sacamos restos, respecto al módulo 21, resulta $d+19u\equiv 0(mód.21)$ o bien $d\equiv 2u(mód.21)$, por lo que se demuestra que $21|N$ si, y sólo si $21|(d+19u)$ *ó* $21|(d-2u)$.
Dado que el número $21=3\cdot 7$ entonces, también $(3,7$ *ó* $21)|N$
Un número es divisible por 31 si, y sólo si:

1. La suma de sus decenas más 28 veces sus unidades es 31 o múltiplo de 31.
2. La diferencia entre sus decenas y 3 veces sus unidades es 0, 31 o múltiplo de 31.

Sea $10d+u\equiv 0(mód.31)$. Si multiplicamos la ecuación por 28 y sacamos restos, respecto al módulo 31, resulta $d+28u\equiv 0(mód.31)$ o bien $d\equiv 3u(mód.31)$, por lo que se demuestra que $31|N$ si, y sólo si $31|(d+28u)$ *ó* $31|(d-3u)$.
De las tres demostraciones podemos deducir que $9p+1=10k$, ya que se establecen las igualdades $9\cdot 11+1=10\cdot 10=100$, $9\cdot 21+1=10\cdot 19=190$ *ó* $9\cdot 31+1=10\cdot 28=280$. Por otra parte, los inversos de los números $10,19$ *y* 28 respecto a los módulos $11,21$ *y* 31 son 1, 2 *y* 3, que forman una progresión aritmética de razón uno y que coinciden con el valor de las decenas de p. Si esto es cierto, un número sería divisible por 101 si, y sólo si:

1. La suma de sus decenas más $101-10=91$ veces sus unidades sea 101 o múltiplo de 101.
2. La diferencia entre sus decenas y 10 veces sus unidades sea 0, 101 o múltiplo de 101.

Sea $N=101^3+202=1\cdot 030\cdot 503$. Como $103050+3\cdot 91=103323=3\cdot 11\cdot 31\cdot 101$ es múltiplo de 101 ó $103050-3\cdot 10=103020=2^2\cdot 3\cdot 5\cdot 17\cdot 101$ también lo es, se demuestra que $101|N$ si, y sólo si $101|(d+91u)$ *ó* $101|(d-10u)$.
Resumimos en el siguiente cuadro lo que acabamos de demostrar:

Criterios de divisibilidad de números con terminación en 1			
N	Divisibilidad	**N**	Divisibilidad
11	$11\|(d+10u)$ *ó* $11\|(d-u)$	**61**	$61\|(d+55u)$ *ó* $61\|(d-6u)$
21	$21\|(d+19u)$ *ó* $21\|(d-2u)$	**71**	$71\|(d+64u)$ *ó* $71\|(d-7u)$
31	$31\|(d+28u)$ *ó* $31\|(d-3u)$	**81**	$81\|(d+73u)$ *ó* $81\|(d-8u)$
41	$41\|(d+37u)$ *ó* $41\|(d-4u)$	**91**	$91\|(d+82u)$ *ó* $91\|(d-9u)$
51	$51\|(d+46u)$ *ó* $51\|(d-5u)$	**101**	$101\|(d+91u)$ *ó* $101\|(d-10u)$

Criterios de divisibilidad de números con terminación en 9, que son complementarios de los números terminados en 1, tales como $9,19,29,39,49,59,69,79,89,99\ldots$
Un número es divisible por 9 si, y sólo si:

1. La suma de sus decenas más sus unidades es 9 o múltiplo de 9.
2. La diferencia entre sus decenas y 8 veces sus unidades es 0, 9 o múltiplo de 9.

Sea $10d+u\equiv 0(mód.9)$. Si sacamos restos de 10 respecto a 9, resulta $d+u\equiv 0(mód.9)$. Si multiplicamos la ecuación por 8 (complemento $9-1=8$) y sacamos restos, respecto al módulo 9, resulta $d-8u\equiv 0(mód.9)$ o bien $d\equiv 8u(mód.9)$, por lo que se demuestra que $9|N$ si, y sólo si $9|(d+u)$ *ó* $9|(d-8u)$.
Un número es divisible por 19 si, y sólo si:

1. La suma de sus decenas más 2 veces sus unidades es 19 o múltiplo de 19.
2. La diferencia entre sus decenas y 17 veces sus unidades es 0, 19 o múltiplo de 19.

Sea $10d+u\equiv 0(mód.19)$. Si multiplicamos la ecuación por 2 y sacamos restos, respecto al módulo 19, resulta $d+2u\equiv 0(mód.19)$ o bien $d\equiv 17u(mód.19)$, por lo que se demuestra que $19|N$ si, y sólo si $19|(d+2u)$ *ó* $19|(d-17u)$.
Un número es divisible por 29 si, y sólo si:

1. La suma de sus decenas más 3 veces sus unidades es 29 o múltiplo de 29.
2. La diferencia entre sus decenas y 16 veces sus unidades es 0, 29 o múltiplo de 29.

Sea $10d+u\equiv 0(mód.29)$. Si multiplicamos la ecuación por 3 y sacamos restos, respecto al módulo 29, resulta $d+3u\equiv 0(mód.29)$ o bien $d\equiv 16u(mód.29)$, por lo que se demuestra que $29|N$ si, y sólo si $29|(d+3u)$ *ó* $29|(d-16u)$.
Como en el caso anterior, se produce una progresión aritmética de razón *1* en el caso de la suma, $\{1,2,3,\cdots\}$ y una progresión aritmética de razón *9* en el caso de la resta, $\{8,17,26\cdots\}$ como se demuestra en la siguiente tabla:

Criterios de divisibilidad de números con terminación en 9			
N	Divisibilidad	**N**	Divisibilidad
9	$9\|(d+u)$ *ó* $9\|(d-8u)$	**59**	$59\|(d+6u)$ *ó* $59\|(d-53u)$
19	$19\|(d+2u)$ *ó* $19\|(d-17u)$	**69**	$69\|(d+7u)$ *ó* $69\|(d-62u)$
29	$29\|(d+3u)$ *ó* $29\|(d-26u)$	**79**	$79\|(d+8u)$ *ó* $79\|(d-71u)$
39	$39\|(d+4u)$ *ó* $39\|(d-35u)$	**89**	$89\|(d+9u)$ *ó* $89\|(d-80u)$
49	$49\|(d+5u)$ *ó* $49\|(d-44u)$	**99**	$99\|(d+10u)$ *ó* $99\|(d-89u)$

Criterios de divisibilidad de números terminados en 3, como $3,13,23,33,43,53,63,73,83,93\ldots$
Un número es divisible por 3 sí, y sólo sí,

1. La suma de sus decenas más sus unidades es 3 o múltiplo 3.
2. La diferencia entre sus decenas y 2 veces sus unidades es 0, 3 o múltiplo de 3.

Sea $10d+u\equiv 0(mód.3)$. Si sacamos restos, respecto al módulo 3, resulta $d+u\equiv 0(mód.3)$ o bien $d\equiv 2u(mód.3)$, por lo que se demuestra que $3|N$ si, y sólo si $3|(d+u)$ *ó* $3|(d-2u)$.
Un número es divisible por 13 si, y sólo si:

1. La suma de sus decenas más 4 veces sus unidades es 13 o múltiplo 13.
2. La diferencia entre sus decenas y 9 veces sus unidades es 0, 13 o múltiplo de 13.

Sea $10d+u\equiv 0(mód.13)$. Si multiplicamos la ecuación por 4 y sacamos restos, respecto al módulo 13, resulta $d+4u\equiv 0(mód.13)$ o bien $d\equiv 9u(mód.13)$, por lo que se demuestra que $13|N$ si, y sólo si $13|(d+4u)$ *ó* $13|(d-9u)$.
Un número es divisible por 23 si, y sólo si:

1. La suma de sus decenas más 7 veces sus unidades es 23 o múltiplo 23.
2. La diferencia entre sus decenas y 16 veces sus unidades es 0, 23 o múltiplo de 23.

Sea $10d+u\equiv 0(mód.23)$. Si multiplicamos la ecuación por 7 y sacamos restos, respecto al módulo 23, resulta $d+7u\equiv 0(mód.23)$ o bien $d\equiv 16u(mód.23)$, por lo que se demuestra que $23|N$ si, y sólo si $23|(d+7u)$ *ó* $23|(d-16u)$.
En este caso, las progresiones son de razón 3, para la suma y de razón 7 para la resta, como se puede observar en la siguiente tabla:

Criterios de divisibilidad de números con terminación en 3			
N	Divisibilidad	**N**	Divisibilidad
3	$3\|(d+u)$ *ó* $3\|(d-2u)$	**53**	$53\|(d+16u)$ *ó* $53\|(d-37u)$
13	$13\|(d+4u)$ *ó* $19\|(d-9u)$	**63**	$63\|(d+19u)$ *ó* $63\|(d-44u)$
23	$23\|(d+7u)$ *ó* $23\|(d-16u)$	**73**	$73\|(d+22u)$ *ó* $73\|(d-51u)$
33	$33\|(d+10u)$ *ó* $33\|(d-23u)$	**83**	$83\|(d+25u)$ *ó* $83\|(d-58u)$
43	$43\|(d+13u)$ *ó* $49\|(d-30u)$	**93**	$93\|(d+28u)$ *ó* $93\|(d-65u)$

Criterios de divisibilidad de números con terminación en 7, que son complementarios de los números terminados en 3, como $7,17,37,47,57,67,77,87,97\ldots$
Un número es divisible por 7 si, y sólo si:

1. La suma de sus decenas más 5 veces sus unidades es 7 o múltiplo 7.
2. La diferencia entre sus decenas y 2 veces sus unidades es 0, 7 o múltiplo de 7

Sea $10d+u\equiv 0(mód.7)$. Si multiplicamos la ecuación por 5 y sacamos restos, respecto al módulo 7, resulta $d+5u\equiv 0(mód.7)$ o bien $d\equiv 2u(mód.7)$, por lo que se demuestra que $7|N$ si, y sólo si $7|(d+5u)$ *ó* $7|(d-2u)$.
Un número es divisible por 17 si, y sólo si:

1. La suma de sus decenas más 12 veces sus unidades es 17 o múltiplo 17.
2. La diferencia entre sus decenas y 5 veces sus unidades es 0, 17 o múltiplo de 17

Sea $10d+u\equiv 0(mód.17)$. Si multiplicamos la ecuación por 12 y sacamos restos, respecto al módulo 17, resulta $d+12u\equiv 0(mód.17)$ o bien $d\equiv 5u(mód.17)$, por lo que se demuestra que $17|N$ si, y sólo si $17|(d+12u)$ *ó* $17|(d-5u)$.
En este caso, las progresiones son de razón 7, para la suma, y de razón 3, para resta. Ver tabla a continuación:

Criterios de divisibilidad de números con terminación en 7			
N	Divisibilidad	**N**	Divisibilidad
7	$7 \mid (d+5u)$ *ó* $7 \mid (d-2u)$	**57**	$57 \mid (d+30u)$ *ó* $57 \mid (d-17u)$
17	$17 \mid (d+12u)$ *ó* $17 \mid (d-5u)$	**67**	$67 \mid (d+47u)$ *ó* $67 \mid (d-20u)$
27	$27 \mid (d+19u)$ *ó* $27 \mid (d-8u)$	**77**	$77 \mid (d+54u)$ *ó* $77 \mid (d-23u)$
37	$37 \mid (d+26u)$ *ó* $37 \mid (d-11u)$	**87**	$87 \mid (d+61u)$ *ó* $87 \mid (d-26u)$
47	$47 \mid (d+33u)$ *ó* $47 \mid (d-14u)$	**97**	$97 \mid (d+68u)$ *ó* $97 \mid (d-29u)$

1.3 ¿Por qué los números primos terminan en 1,3,7 ó 9? .

Esta pregunta se la hizo allá por el año 1741 el más prolífico, fuera de toda comparación y de todos los matemáticos: Leonhard Euler (1707-1783). Pensó que nuestro sistema de numeración basado en el número 10 tendría la respuesta. El 10 se factoriza como $10 = 2 \cdot 5$. Si un número se divide entre 10 pueden ocurrir dos cosas:
Si el número es 10 o múltiplo de 10, no hay resto, luego

$$\frac{N}{10} = 10q$$

Si el número no es múltiplo de 10, se produce un resto, luego

$$\frac{N}{10} = 10q + r \text{ donde } r \text{ puede tomar los valores de } r = 1,2,3,4,5,6,7,8,9$$

Esto es lo que se conoce como sistema completo de restos respecto a un número.
A continuación comprobó cuántos de estos restos son coprimos con 10, de tal forma que $mcd(10,r) = 1$ y encontró que el $mcd\left(10,\{1,2,3,4,5,6,7,8,9\}\right) = 1,3,7,9$
Ya tenía la prueba de las terminaciones y, además, la excepcionalidad de los primos 2 y 5, que son primos por sí solos y no en compañía de otros.
Esta demostración es la que hoy se conoce como función de Euler, $\varphi(n)$.

2. 2. *Factorización.*

2.1 Concepto de factorización.

El teorema fundamental de la aritmética nos dice que, *todo entero distinto de cero puede ser expresado como el producto de* ± 1 *por factores primos positivos*. Esta expresión es *única*, salvo el orden en que los factores se consideren. La descomposición canónica del número N en factores primos vendría determinada por

$$N = p_1^{\alpha} \cdot p_2^{\beta} \cdot \ldots \cdot p_n^{\gamma}$$

Decimos que, un entero p es primo si, siendo distinto de 0 y de ± 1, es divisible *únicamente* por ± 1 *y* $\pm p$. Un número que sea distinto de 0 y ± 1 y que no sea primo, se llama *compuesto.* Una representación de números la tenemos en

2,3,5,7,11,13,17,19,23,29,31,37,41,43,47,53,59,61,67,71,73,79,
83,89,97,101,103,107,109,113,127,131,137,139,149,151,157,163

Todo número m compuesto, $m \in \mathbb{Z}$, admite, al menos, un divisor primo distinto de 1, ya que los divisores de un número son menores o iguales a dicho número, por tanto su cantidad es infinita.

Todo número m compuesto, $m \in \mathbb{Z}$, puede expresarse mediante el producto de factores primos.

Si $m \in \mathbb{Z}$ es compuesto, entonces existe un primo p tal que $p \mid m$ y $p \leqq \sqrt{m}$.

En la práctica, para descomponer un número en factores primos, se divide el número por el menor de sus divisores primos, el cociente resultante se vuelve a dividir por el menor de sus divisores primos y así sucesivamente, hasta obtener como cociente un número primo.

Ejemplo: descomponer en factores primos el número 23205.

Previamente, analicemos el número:

Los divisores, si los tiene, serán $\sqrt{23205} \leqq 152$.

No es divisible por 2 porque no termina ni en 0 ni en cifra par.

Es divisible por 3 porque la suma de sus cifras es 3 o múltiplo de 3:

$2+3+2+0+5=12 \rightarrow 1+2=3$

Es divisible por 5 porque termina en 5.

Es divisible por 7 porque $2320+5\cdot 5=2345,\ 234+5\cdot 5=259,\ 25+5\cdot 9=70,$ o bien porque $2320-2\cdot 5=2310,\ 23-2\cdot 1=21,\ 2-2\cdot 1=0.$

No es divisible por 11 porque $2320-5=2315,\ 231-5=226,\ 22-6=16$ y 16 no es ni 0, ni 11 ni múltiplo de 11.

Es divisible por 13 porque $2320-9\cdot 5=2275,\ 227-9\cdot 5=182,\ 18-9\cdot 2=0.$

Es divisible por 17 porque $2320-5\cdot 5=2295,\ 229-5\cdot 5=204,\ 20-5\cdot 4=0.$

Podemos decir que $23205=3\cdot 5\cdot 7\cdot 13\cdot 17.$ Probemos su desarrollo de forma práctica:

23205	
23205	3
7735	5
1547	7
221	13
17	17
1	

$23205=3\cdot 5\cdot 7\cdot 13\cdot 17$

2.2 Máximo Común Divisor $mcd(a,b)=d$.

Dados dos números enteros no nulos a y b, cualquier entero que los divida a ambos es lo que se llama, un *divisor común*. El mayor de ellos es el *Máximo Común Divisor* de esos dos enteros, que expresamos como $mcd(a,b)=d$. El mcd de a y b será divisible por cualquier otro divisor común a dichos números. Si se conoce la descomposición en factores primos de a y b, su mcd se obtiene inmediatamente, como *producto de los factores primos comunes afectado cada uno de ellos del mayor exponente*.

Algunas de las propiedades del máximo común divisor son:

1. Si dos números cualesquiera se multiplican o dividen por un mismo número, su mcd queda multiplicado o dividido, respectivamente, por dicho número.
2. Si un número divide a un producto de dos factores y es primo con uno de ellos, también dividirá al otro.
3. Los divisores comunes de dos números son los divisores de su mcd.
4. Los cocientes de dividir dos números por su mcd son primos entre sí.

Para hallar el mcd de dos números podemos establecer el siguiente procedimiento:
Se divide el mayor por el menor y, si la división es exacta, el menor es el mcd *de ambos. Si queda resto, se divide el divisor por el resto y se continúa partiendo siempre el divisor por el resto, hasta obtener división exacta. El último divisor es el* mcd *de los dos números*. Este procedimiento, conocido como *Algoritmo de Euclides*, se basa en que, dados dos números *a* y *b* con $b>0$, existe un único par de enteros *q* y *r* tales que $a=bq+r$, con $0\le r<b$ donde $q\ y\ r$ son, respectivamente, el cociente y el resto de dividir *a por b*. Este procedimiento queda reflejado como sigue:

$$\begin{array}{ll} a=bq_1+r_1 & 0<r_1\le b \\ b=r_1q_2+r_2 & 0<r_2\le r_1 \\ r_1=r_2q_3+r_3 & 0<r_3\le r_2 \\ \quad\ldots\ldots & \quad\ldots\ldots \\ r_{n-2}=r_{n-1}q_n+r_n & 0<r_n\le r_{n-1} \\ r_{n-1}=r_nq_n+0 & \end{array}$$

Según *Euclides* existen dos enteros, $s\ y\ t$ tales que, $mcd(a,b)=d=as+bt$. La llamada Identidad de Bézout dice que, si $a\ y\ b$ son dos números enteros tales que al menos uno de ellos es distinto de cero, entonces existen enteros $x_0,y_0\in\mathbb{Z}$ tales que el

$$mcd(a,b)=d=ax_0+by_0.$$

Ejemplo: Calcular el mcd de 759 y 345.
Empecemos por factorizar los números propuestos:
El número 759 es divisible por 3, ya que $7+5+9=21,\ 2+1=3$. Como $759/3=253$ y vemos que $25-3=22,\ 2-2=0,$ también es divisible por 11, por lo que $759=3\cdot11\cdot23$.
El número 345 es divisible por 5, ya que termina en 5. Como $345/5=69$ que claramente se ve es múltiplo de 3, tenemos $345=3\cdot5\cdot23$.
Los factores comunes de ambos números son $345=\underline{3}\cdot5\cdot\underline{23}$ y $759=\underline{3}\cdot11\cdot\underline{23}$ esto es, el 3 y el 23, por tanto $mcd(345,759)=3\cdot23=69$.
Si utilizamos el *Algoritmo de Euclides*:

$$\begin{array}{l} 759=345\cdot2+69 \\ 345=69\cdot5+0 \qquad mcd(345,759)=69 \\ \ 69=0 \end{array}$$

En cuanto a los coeficientes Bézout, como en el desarrollo hemos obtenido los multiplicadores 2 y 5, utilizando fracciones continuas resultan:

	2	5
0 1	2	11
1 0	1	5

$mcd(345,759)=69=345(-2)+759(1)$

2.3 Mínimo Común Múltiplo $mcm(a,b)=m$.

Dados dos números enteros no nulos *a* y *b*, cualquier entero que sea múltiplo de ambos es lo que se llama, un *múltiplo común*. El menor de todos los positivos es el *Mínimo Común Múltiplo* de esos dos enteros, que expresamos como $mcm(a,b)=d$. El mcm de *a* y *b* será divisor de

cualquier otro múltiplo común a dichos números. Si se conoce la descomposición en factores primos de *a* y *b*, su mcm se obtiene inmediatamente como *producto de los factores primos comunes y no comunes afecto cada uno de ellos del mayor exponente*.
Existe una forma que relaciona a,b con D,M donde *a y b* son números cualesquiera y D *y* M representan el mcd y mcm, respectivamente, produciéndose la igualdad matemática, $ab=DM$, que nos permite conocer cualquiera de ellos en función del otro.
Algunas de las propiedades del mínimo común múltiplo son:

1. Si cualquiera de los números en cuestión es múltiplo de los demás, él es el mcm.
2. Si los números en cuestión son primos entre sí, el producto de todos ellos es el mcm.
3. Cualquier múltiplo del mcm es también un múltiplo común.
4. Si los números en cuestión se multiplican o dividen por un mismo número, su mcm queda multiplicado o dividido por dicho número.
5. Si se divide al mcm de varios números por cada uno de ellos, sus cocientes son primos entre sí.

Existe una forma que relaciona a,b con D,M donde *a y b* son números cualesquiera y D *y* M representan el mcd y mcm, respectivamente, produciéndose la igualdad matemática, $ab=DM$, que nos permite conocer cualquiera de ellos en función del otro.
Ejemplo: Calcular el mínimo común múltiplo de los números 378, 468 y 1176.
Por simple observación, el 378 es divisible por 2,3 y 7, luego $378/(2\cdot 3\cdot 7)=378/42=9$. El número $9=3^2$, lo que nos permite deducir que $378=2\cdot 3^3\cdot 7$.
El número 468 es divisible por 2 y por 3, luego $468/(2\cdot 3)=468/6=78$. El número $78=2\cdot 3\cdot 13$, lo que nos permite deducir que $468=2^2\cdot 3^2\cdot 13$.
El número 1176 es divisible por 2,3 y 7, entonces $1176/(2\cdot 3\cdot 7)=1176/42=28$. El número $28=2^2\cdot 7$, por lo que deducimos que $1176=2^3\cdot 3\cdot 7^2$.
Los factores primos, comunes y no comunes, afectados cada uno de ellos del mayor exponente son el $2^3,3^3,7^2,13$ por tanto,

$$\left.\begin{array}{r} 378=2\cdot 3^3\cdot 7 \\ 468=2^2\cdot 3^2\cdot 13 \\ 1176=2^3\cdot 3\cdot 7^2 \end{array}\right\} \; mcm(378,468,1176)=2^3\cdot 3^3\cdot 7^2\cdot 13=137592$$

Si relacionamos mcd con mcm,

$$abc=DM,\ \ \mathrm{D}=\frac{\mathrm{abc}}{\mathrm{M}}=\frac{378\cdot 468\cdot 1176}{137592(2^2\cdot 3^2\cdot 7)}=\frac{208039104}{34673184}=6$$

$$abc=DM,\ \ \mathrm{M}=\frac{\mathrm{abc}}{\mathrm{D}}=\frac{378\cdot 468\cdot 1176}{6(2^2\cdot 3^2\cdot 7)}=\frac{208039104}{1512}=137592$$

Cuando el mcd o mcm lo componen más de dos números, deben añadirse al denominador el producto de los coeficientes no utilizados.
El $mcd(378,468,1176)=2\cdot 3=6$, el $mcm(378,468,1176)=2^3\cdot 3^3\cdot 7^2\cdot 13=137592$, quedan libres el $2^2\cdot 3^2\cdot 7=252$, que debemos añadir al dominador para compensar el producto de los tres números que intervienen.

2.4 Hallar un procedimiento para calcular el número de divisores de un número.

El número de divisores de un número vendrá determinado por los factores primos que contenga la descomposición factorial del mismo. Si tenemos en cuenta que esta descomposición es $N = p_1^{\alpha} \cdot p_2^{\beta} \cdot \ldots \cdot p_n^{\gamma}$ el número de divisores vendrá determinado por:

$$\tau_{(n)} = (\alpha+1)(\beta+1)(\gamma+1)\cdots$$

Ejemplo: Calcular el número de divisores de 720.
La descomposición factorial de $720 = 2^4 \cdot 3^2 \cdot 5$, por tanto

$$\tau_{(720)} = (4+1)(2+1)(1+1) = 5 \cdot 3 \cdot 2 = 30$$

2.5 Hallar un procedimiento para calcular los divisores de un número.

A partir de la descomposición factorial de un número, para conocer sus divisores se utiliza la siguiente regla:
Se escriben la unidad y las potencias sucesivas del primer factor simple y estos números se multiplican por las potencias sucesivas del segundo factor primo. Se multiplican todos los números obtenidos por las potencias sucesivas del tercer factor simple; después, todos los números obtenidos por las potencias sucesivas del cuarto factor simple y, se continúa del mismo modo hasta emplear las potencias sucesivas del último factor simple. Los números así hallados serán todos divisores del número propuesto.
Ejemplo: Hallar los divisores de los $a)\ 252, b)\ 1078, c)\ 1750\ y\ d)\ 29645$.
Como

$$a)\ \tau_{(252)} = (2+1)(2+1)(1+1) = 18,$$

$$b)\ \tau_{(1078)} = (1+1)(2+1)(1+1) = 12,$$

$$c)\ \tau_{(1750)} = (1+1)(3+1)(1+1) = 16,$$

$$d)\ \tau_{(29645)} = (1+1)(2+1)(2+1) = 18.$$

identificamos los divisores mediante las siguientes tablas:

$252 = 2^2 \cdot 3^2 \cdot 7$		
1	2	4
3	6	12
9	18	36
7	14	28
21	42	84
63	126	252

$1078 = 2 \cdot 7^2 \cdot 11$	
1	2
7	14
49	98
11	22
77	154
539	1078

$1750 = 2 \cdot 5^3 \cdot 7$	
1	2
5	10
25	50
125	250
7	14
35	70
175	350
875	1750

$29645 = 5 \cdot 7^2 \cdot 11^2$	
1	5
7	35
49	245
11	55
77	385
539	2695
121	605
847	4235
5929	29645

2.6 Hallar un procedimiento para calcular la suma de los divisores de un número.

Si tenemos en cuenta que el número de divisores de un número viene determinado por $\tau_{(n)} = \alpha + 1,$ la suma de dichos divisores sería:

$$\sigma_{(n)} = \frac{a^{\alpha+1}-1}{a-1} \cdot \frac{b^{\beta+1}-1}{b-1} \cdot \frac{c^{\gamma+1}-1}{c-1} \cdots$$

Fórmula desarrollada por Euler que relaciona el número de divisores con la suma del número que los genera.
Ejemplo: Hallar la suma de divisores de los $a)\ 252, b)\ 1078, c)\ 1750\ y\ d)\ 29645.$
Primero factorizamos los números propuestos:

$$a)\ 252 = 2^2 \cdot 3^2 \cdot 7^1,$$

$$b)\ 1078 = 2^1 \cdot 7^2 \cdot 11^1,$$

$$c)\ 1750 = 2^1 \cdot 5^3 \cdot 7^1,$$

$$d)\ 29645 = 5^1 \cdot 7^2 \cdot 11^2,$$

luego, la suma de sus divisores más el propio número sería

$$a)\ \sigma_{(252)} = \frac{2^{2+1}-1}{2-1} \cdot \frac{3^{2+1}-1}{3-1} \cdot \frac{7^{1+1}-1}{7-1} = 728 = 476 + 252;$$

$$b)\ \sigma_{(1078)} = \frac{2^{1+1}-1}{2-1} \cdot \frac{7^{2+1}-1}{7-1} \cdot \frac{11^{1+1}-1}{11-1} = 2052 = 974 + 1078;$$

$$c)\ \sigma_{(1750)} = \frac{2^{1+1}-1}{2-1} \cdot \frac{5^{3+1}-1}{5-1} \cdot \frac{7^{1+1}-1}{7-1} = 3744 = 1994 + 1750;$$

$$d)\ \sigma_{(29645)} = \frac{5^{1+1}-1}{5-1} \cdot \frac{7^{2+1}-1}{7-1} \cdot \frac{11^{2+1}-1}{11-1} = 45486 = 15841 + 29645.$$

2.7 Hallar un procedimiento para calcular el producto de los divisores de un número.

Consiste en hallar el producto de todos los divisores de un número $N = p_1^{\alpha} \cdot p_2^{\beta} \cdot \ldots \cdot p_n^{\gamma},$ que cuantificamos como $\tau_{(n)} = (\alpha+1)(\beta+1)\cdot\ldots\cdot(\gamma+1)$ y que podemos expresar como

$$P^n = \pi = \sqrt{N^{\tau}}$$

Ejemplo: Hallar el producto de los divisores de $a)\ 51, b)\ 30\ y\ c)\ 100.$
Empecemos por calcular la descomposición factorial y el número de divisores de cada uno de los números propuestos:

$$a)\ 51 = 3^1 \cdot 17^1 \mapsto \tau_{(51)} = (1+1)(1+1) = 4;$$
$$b)\ 30 = 2^1 \cdot 3^1 \cdot 5^1 \mapsto \tau_{(30)} = (1+1)(1+1)(1+1) = 8;$$
$$c)\ 100 = 2^2 \cdot 5^2 \mapsto \tau_{(100)} = (1+2)(1+2) = 9.$$

Ahora, el producto de sus divisores sería:

$$a)\ \sqrt{51^4} = 51^2 = 2601;$$

$$b)\ \sqrt{30^8} = 30^4 = 810 \cdot 000;$$

$$c)\ \sqrt{100^9} = 100^{4,5} = 1 \cdot 000 \cdot 000 \cdot 000$$

2.8 Calcular la suma de los divisores de 220 y 284.

La descomposición factorial es

$$220 = 2^2 \cdot 5 \cdot 11 \text{ y } 284 = 2^2 \cdot 71$$

El número de divisores

$$\tau_{(220)} = (2+1)(1+1)(1+1) = 12 \text{ y}$$

$$\tau_{(284)} = (2+1)(1+1) = 6.$$

La suma de sus divisores,

$$\sigma_{(220)} = \frac{2^{2+1}-1}{2-1} \cdot \frac{5^{1+1}-1}{5-1} = 504 = 284 + 220 \text{ y}$$

$$\sigma_{(284)} = \frac{2^{2+1}-1}{2-1} \cdot \frac{71^{1+1}-1}{71-1} = 504 = 220 + 284$$

Obtenemos la misma suma. *Son números amigos*.
Dos números son amigos si la suma de los divisores de cada uno de ellos, excluyendo los propio es igual al del otro.
Eran conocidos por los griegos del siglo VI antes de Cristo. Hacia el año 1638, Fermat pone en práctica una regla que había sido descubierta por Thabit Ibn Qurra en el siglo IX, en la que afirmaba que para que cualquier número *n* y *m* sean amigos, basta que se descompongan en la forma

$$\left.\begin{array}{l} n = 2^p \cdot q \cdot r \\ m = 2^p \cdot s \end{array}\right\} \text{ en donde } q, r, s \text{ son primos de la forma } \left\{\begin{array}{l} q = 3 \cdot 2^{p-1} - 1 \\ r = 3 \cdot 2^p - 1 \\ s = 9 \cdot 2^{2p-1} - 1 \end{array}\right. .$$

Para nuestro supuesto, que aparece en la Biblia (Génesis 32,14), donde Jacob ofrece a su hermano 220 ovejas cuando pensaba que lo iba a matar, si hacemos que *n = 2*, obtenemos para

$$q = 3 \cdot 2^{2-1} - 1 = 5,\ r = 3 \cdot 2^2 - 1 = 11 \text{ y } s = 9 \cdot 2^{2 \cdot 2-1} - 1 = 71$$

y resulta para

$$n = 2^2 \cdot 5 \cdot 11 = 220 \text{ y } m = 2^2 \cdot 71 = 284$$

Estos números también aparecen con frecuencia en los escritos árabes. Ibn Jaldún (1332,1406), en su *Prolegómeno Histórico*, les reconoce virtudes maravillosas para la confección de talismanes y horóscopos y también habla de sus propiedades mágicas. En Europa, autores del siglo XVI como Chuquet, Étienne de la Roche, Cardano o Tartaglia escribieron sobre estos números. Pero fue Fermat (1601-1665) el primero capaz de obtener un nuevo par de números amigos: 17296 y 18416. Su publicación y el desafío a Descartes (1596-1650) instándole a encontrar otra pareja, hace que dos años después éste consiguiera la pareja compuesta por 9363584 y 9437056. Euler (1707-1783), el matemático suizo conocido como el *"maestro de todos los matemáticos"*, consiguió en 1747, una lista de treinta parejas.

2.9 Calcular la suma de los divisores de 6 y 28.

Los divisores de 6 son 1, 2, 3, que suman 6. Los divisores de 28 son 1, 2, 4, 7, 14, que suman 28. Cuando la suma de divisores es igual al número que las produce, se dice que son *números perfectos*.
Conocidos desde la antigüedad, tenían una interpretación divina y fueron introducidos en Occidente por Pitágoras. San Agustín (354-430 a.C.), en su libro *La Ciudad de Dios*, afirma que el 6 es perfecto porque Dios hizo el Mundo en seis días. Por otra parte, la civilización sumeria consideraba perfecto al número veintiocho porque la luna tardaba ese tiempo en dar una vuelta entera alrededor de la Tierra. Euclides los menciona en sus Elementos (IX, 36), pero es a partir del siglo XII cuando, desde Fibonacci hasta Euler, dedicaron más tiempo a su estudio. Precisamente Euler, sobre la base de los números primos de Mersenne, creó un método por el que permite conocer si un número es o no perfecto.
Tabla de alguno de los números perfectos conocidos:

n	2^{n-1}	*Primo de Mersenne* $M_{(n)} = 2^n - 1$		*Número Perfecto* $P_{(n)} = 2^{n-1}(2^n - 1)$	
2	2^{2-1}	3	$2^2 - 1$	$2^{2-1}(2^2 - 1)$	6
3	2^{3-1}	7	$2^3 - 1$	$2^{3-1}(2^3 - 1)$	28
5	2^{5-1}	31	$2^5 - 1$	$2^{5-1}(2^5 - 1)$	496
7	2^{7-1}	127	$2^7 - 1$	$2^{7-1}(2^7 - 1)$	8128
13	2^{13-1}	8091	$2^{13} - 1$	$2^{13-1}(2^{13} - 1)$	33550336

Los cuatro primeros números perfectos, 6, 28, 496, 8128, aparecen ya en la *Introductio Arithméticae* de Nicómaco de Gerasa (hacia el año 100 d.C.).
El quinto número perfecto, 33.550.336, aparece en un manuscrito del siglo XV.
Los números perfectos sexto y séptimo, 8.589.869.056, 137.438.691.328, fueron descubiertos en 1588 por Pedro Antonio Cataldi (1548-1626).
Siempre que se descubre un nuevo número primo de Mersenne del tipo $2^n - 1$, se puede generar un nuevo número perfecto sólo con multiplicarlo por 2^{n+1}. Así, en 1772, Euler demostró que el 2.305.843.008.139.952.128 era el octavo número perfecto al demostrar que $2^{31} - 1$ era el 2.147.483.647, octavo primo de Mersenne.
Los números perfectos están íntimamente vinculados con la suma de cubos. Por ejemplo:

$$\sum_{n}^{2}(2n-1)^3 = 1^3 + 3^3 = 28$$

$$\sum_{n}^{4}(2n-1)^3 = 1^3 + 3^3 + 5^3 + 7^3 = 496$$

$$\sum_{n}^{8}(2n-1)^3 = 1^3 + 3^3 + 5^3 + 7^3 + 9^3 + 11^3 + 13^3 + 15^3 = 8128$$

$$\sum_{n}^{64}(2n-1)^3 = 33 \cdot 550 \cdot 336$$

$$\sum_{n}^{256}(2n-1)^3 = 85 \cdot 89 \cdot 869 \cdot 056$$

$$\sum_{n}^{512}(2n-1)^3 = 137 \cdot 438 \cdot 691 \cdot 328$$

2.10 Aplicando el teorema de Fermat, demostrar que 13837 y 2027651281 son números primos.

La raíz cuadrada de 13837 está comprendida entre 117 y 118, sin embargo $118^2 - 13837 = 87$ no es un cuadrado perfecto. Probamos con $119^2 - 13837 = 324$ que sí lo es, luego

$$13837 = 119^2 - 18^2 = (119-18)(119+18) = 101 \cdot 137$$

que nos confirma que el 13837 no es un número primo.
El número 2027651281 fue utilizado por Fermat para demostrar la efectividad de su método. Su raíz cuadrada está comprendida entre 45029 y 45030 y los sucesivos números probados se recogen en la siguiente tabla:

x	$x^2 - n$	x	$x^2 - n$
45030	49619	45036	590015
45031	139680	45037	680088
45032	229743	45038	770163
45033	319808	45039	860240
45034	409875	45040	950319
45035	499944	45041	1040400

El último número encontrado, 1040400 es cuadrado perfecto de 1020, con lo que tenemos, $2027651281 = 45041^2 - 1020^2 = (45041+1020)(45041-1020) = 46061 \cdot 44021$, que demuestra que el número propuesto no es primo.

2.11 Aplicando criterios de Euler-Fermat, determinar si son o no primos los números 2257 y 42319.

La divisibilidad de números grandes requiere herramientas más potentes que las ofrecidas por Fermat, precisamente, basándose en éste, Euler nos dejó el siguiente teorema. *Si a es un número par y p es un número primo que no es factor de a pero sí divisor exacto de* $a+1$ *en-*

tonces, para cierto número k, $p = 2k + 1$. A partir de estos argumentos se puede establecer que:

Si p divide a $a + 1$,	p tiene la forma de $2k + 1$
Si p divide a $a^2 + 1$,	p tiene la forma de $4k + 1$
Si p divide a $a^4 + 1$,	p tiene la forma de $8k + 1$
Si p divide a $a^8 + 1$,	p tiene la forma de $16k + 1$
Si p divide a $a^{16} + 1$,	p tiene la forma de $32k + 1$
Si p divide a $a^{32} + 1$,	p tiene la forma de $64k + 1$
Si p divide a $a^{64} + 1$,	p tiene la forma de $128k + 1$

y en general, *si p divide exactamente* $a \cdot a^{2n} + 1$, *entonces,* $p = (2^{n+1})k + 1$, *para todo número entero de k*.
Siguiendo este criterio y teniendo en cuenta que los números propuestos son de la forma $4k + 1$, tenemos que:

2257		**42319**	
$1 \cdot 4 + 1 =$	5 primo no divisible por 2257.	$10 \cdot 4 + 1 =$	41 primo no divisible
$2 \cdot 4 + 1 =$	9 número compuesto	$11 \cdot 4 + 1 =$	45 número compuesto
$3 \cdot 4 + 1 =$	13 primo no divisible por 2257	$12 \cdot 4 + 1 =$	49 número compuesto
$4 \cdot 4 + 1 =$	17 primo no divisible por 2257	$12 \cdot 4 + 1 =$	53 primo no divisible
$5 \cdot 4 + 1 =$	21 número compuesto	$13 \cdot 4 + 1 =$	57 número compuesto
$6 \cdot 4 + 1 =$	25 número compuesto	.....	.....
$7 \cdot 4 + 1 =$	29 primo no divisible por 2257	$23 \cdot 4 + 1 =$	93 número compuesto
$8 \cdot 4 + 1 =$	33 número compuesto	$24 \cdot 4 + 1 =$	97 primo no divisible
$9 \cdot 4 + 1 =$	37 primo divisible por 2257	$25 \cdot 4 + 1 =$	101 número divisible

Se trata de dos números compuestos, $2257 = 37 \cdot 61 \, y \; 42319 = 101 \cdot 419$.

2.12 Teniendo en cuenta lo dicho por Fermat, que todos los números primos de la forma $4k + 1$ se pueden expresar como suma de dos cuadrados, probar si es cierto con los números 5, 13, 17, 61 y 65.

Efectivamente, para los primos $5 = 2^2 + 1^2$, $13 = 2^2 + 3^2, 17 = 4^2 + 1^2, 61 = 5^2 + 6^2$ se cumple perfectamente, pero también para $65 = 4^2 + 7^2$, que como se puede comprobar, es número compuesto.
$Diofanto\ de\ Alejandría$ ya usó estas formas que nos permiten saber que el producto de dos números que son suma de dos cuadrados es también una suma de dos cuadrados, esto es

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

Si este procedimiento lo aplicamos a los números 61 y 65, tendremos

$$61 \cdot 65 = (6^2 + 5^2)(4^2 + 7^2) = (6 \cdot 4 + 5 \cdot 7)^2 + (6 \cdot 7 - 5 \cdot 4)^2 = (24 + 35)^2 + (42 - 20)^2$$

y finalmente: $61 \cdot 65 = 59^2 + 22^2$

2.13 Según Fermat, el número $2^{32}+1$ es número primo ¿tenía razón?

No, no la tenía. A Euler le costó siete años refutar la conjetura de Fermat mediante su gran teorema que hemos esbozado en el supuesto 2.11.
El número $2^{32}+1=4294967297$ no es primo, es divisible por 641.
Demostración de Euler: Puesto que $a=2$ es ciertamente par, se demuestra que cualquier factor primo $2^{32}+1$ debe tener la forma $p=64k+1,$ donde *k* es un número entero y por tanto:

Si $k=1,\ 64k+1=65$	Que no es primo.
Si $k=2,\ 64k+1=129$	Que no es primo.
Si $k=3,\ 64k+1=193$	Es primo pero no divisible por $2^{32}+1.$
Si $k=4,\ 64k+1=257$	Es primo pero no divisible por $2^{32}+1.$
Si $k=5,\ 64k+1=321$	Que tampoco es primo.
Si $k=6,\ 64k+1=385$	Que tampoco es primo.
Si $k=7,\ 64k+1=449$	Es primo pero no divisible por $2^{32}+1.$
Si $k=8,\ 64k+1=513$	Que no es primo.
Si $k=9,\ 64k+1=577$	Es primo pero no divisible por $2^{32}+1.$
Si $k=10,\ 64k+1=641$	Número primo divisible por $2^{32}+1.$

Euler no sólo demostró que no era primo, sino que, además

$$2^{32}+1=(2^2)(2^{30})+1=4(1073741824)+1$$

tiene la forma $64k+1$ y por tanto, posee un modo único de descomposición factorial en la suma de dos cuadrados, esto es

$$2^{32}+1=65536^2+1^2 \text{ y } 2^{32}+1=20449^2+62264.^2$$

2.14 Explicar la diferencia entre números abundantes y deficientes.

Los números abundantes son un entero natural *n* tal que $n<\sigma(n)$ donde $\sigma(n)$ es la suma de los divisores de *n* distintos de *n*, por ejemplo, *12, 18, 20* son abundantes ya que los divisores de *12* son *1 +2 +3 +4 +6 = 16 > 12*; los de *18* son*, 1 +2 +3 +6 +9 = 21 > 18* y del *20, 1 +2 +4 +5 +10 = 22 > 20.* Todos los múltiplos de *6* estrictamente superiores a *6* son abundantes. El menor abundante impar es el *10665* y todo entero superior a *83160* es la suma de números abundantes.
A diferencia de los abundantes, los números deficientes son enteros naturales estrictamente superiores a la suma de sus divisores que le son estrictamente inferiores. Así, por ejemplo*, 4, 8, 9, 10, 14 y 15* son números deficientes.

2. 3. *Descomposición en suma de factores primos.*

3.1 Goldbach y sus conjeturas.

Christian Goldbach (1690-1764), fue un matemático prusiano, hijo de un pastor, que estudió leyes y matemáticas y conoció a varios famosos de su tiempo como Leibniz, Euler o Daniel

Bernoulli. En 1725 se convirtió en historiador y profesor de matemáticas en San Petersburgo. Tres años después se trasladó a Moscú para trabajar para el zar Pedro II.
Aunque realizó importantes trabajos en el campo de las matemáticas, Goldbach es más conocido por sus conjeturas, conocidas como *Conjeturas de Goldbach*.
Se conoce como Conjetura fuerte de Goldbach la que dice que *todo número par mayor de 2 puede escribirse como suma de dos números primos*. Se puede emplear dos veces el mismo número. Esta conjetura había sido conocida por Descartes. En 1742, en una carta de Goldbach a Euler, le dice que *todo entero impar mayor que 5 se puede escribir como suma de tres números primos*. Esta conjetura se conoce como Conjetura débil de Goldbach. Hay una tercera conjetura que dice que *todo número impar mayor que 7 puede expresarse como suma de tres números primos impares*. Subyace en esta conjetura que no debe utilizarse el 2, único primo par.
Muchos han sido los matemáticos que han intentado su demostración, Hardy, Littlewood, Riemann, entre otros, pero a pesar de los avances llevados a cabo por Vinogradov, Chen o Vaugham, las conjeturas siguen abiertas.
Iván Matvéevich Vinogradov (1891-1983) dice que, de ser cierta la conjetura de Goldbach, resulta inmediatamente que todo número par que 5 es suma de tres números primos. En efecto, si $n \geqq 7$, $n-3$ será par ya que, por la hipótesis de $n-3=p+q,\ p,q \in primos$, tenemos para $n=p+q+3$.
Algunos ejemplos:

Número par mayor de dos:

$$10=3+7=5+5$$
$$20=3+17=7+13$$
$$30=7+23=11+19=13+17$$

Número impar mayor que cinco o mayor que siete:

$$7=2+2+3,\ 9=2+2+5,\ 11=2+3+5$$
$$51=3+7+41=5+17+29=11+17+23$$
$$111=13+19+79=19+31+61=23+29+59$$

Siguiendo la estela Goldbach, he aquí algunas conjeturas sobre los números primos:
$Alphonse\ de\ Polignac\ (1817\ -1890)$ dice que *todo número impar es la suma de un número primo y una potencia de dos:*

$$7=3+2^2=5+2^1,\ 11=3+2^3=7+2^2$$
$$15=7+2^3=11+2^2=13+2^1$$
$$21=5+2^4=13+2^3=17+2^2=19+2^1$$

$A.\ Desboves\ (1855-¿?)$ dice que *cuando un número par es de la forma* $2(2k+1)$, *es simultáneamente igual a la suma de dos números primos de la forma* $4k+1$ *y dos números primos de la forma* $4k-1$, *a cuyo efecto debe considerarse el número 1 como primo*:

Números de la forma $2(2k+1)$

6	10	14	18	22	26	30	34	38	42	46	50	62	66	70

Primos de la forma $4k+1$

5	13	17	29	37	41	53	61	73	89	97	101	109	113	129

Primos de la forma $4k-1$

3	7	11	19	23	31	43	47	59	67	71	79	83	103	107

$18=5+13=11+7,\ 30=11+19=13+17,\ 42=5+37=19+23$
$50=13+37=19+31,\ 94=11+83=41+53,\ 106=17+89=23+83$

Johannes Gualtherus van der Corput $(1890-1975)$ dice *que todo entero impar admite infinitas representaciones de la forma* $p+q-r$, *donde* p,q,r *son primos*:

$1=3+5-7=5+13-17=11+31-41$
$5=23+43-61=29+37-61=23+71-89$
$51=59+71-79=53+71-73=71+89-109$
$99=103+109-113=211+241-353=439+811-1151$

Ching Jun Chen (1933-) dice que *todo número par suficientemente grande es, bien suma de dos enteros primos bien suma de un número primo y del producto de dos números primos*:

$2n=p+q,\ p,q\in primos$	$2n=p+q\cdot r,\ p,q,r\in primos$
$444=167+277$	$444=53+17\cdot 23$
$680=331+349$	$680=13+23\cdot 29$
$1008=499+509$	$1008=19+23\cdot 43$
$1902=911+991$	$1902=139+41\cdot 43$

3.2 La composición de las sumas de números primos.

Sabemos que, salvo las excepciones del $2\ y\ 5$, todos los primos conocidos terminan en $1,3,7\ ó\ 9$. Entre los números 1 y 1000 hay 168 números primos, como podemos comprobar por la tabla siguiente,

2,*3,5,7,11,13,17,19*,23,*29,31*,37,*41,43*,47,53,*59,61*,67,*71,73*,79,83,89,97,*101,103,107,109*,113,127,
131, *137,139,149,151*,157,163,167,173,*179,181,191,193,197,199*,211,223,*227,229*,233,*239,241*,251,
257,263,*269,271*,277,*281,283*,293,307,*311,313*,317,331,337,*347,349*,353,359,367,373,379,383,389,
397,401,409,*419,421,431,433*,439,443,449,457,*461,463*,467,479,487,491,499,503,509,*521,523*,541,
547,557,563,*569,571,*577,587,593,*599,601*,607,613,*617,619*,631,*641,643*,647,653,*659,661*,673,677,
683,691,701,709,719,727,733,739,743,751,757,761,769,773,787,797,809,811,*821,823,827,829*,839,
853,*857,859*,863,877,*881,883*,887,907,911,919,929,937,941,947,953,967,971,977,983,991,997

Si le dedicamos algunos minutos a esta lista, podemos sustraer interesante información:

	CENTENAS										
Hasta	99	199	299	399	499	599	699	799	899	999	Total
Gemelos	7	5	2	2	2	1	1	0	4	0	24

Terminación en 1	5	5	5	2	5	3	5	3	3	4	40
Terminación en 2	1										1
Terminación en 3	7	5	5	4	3	4	5	3	4	2	42
Terminación en 5	1										1
Terminación en 7	6	6	3	6	3	4	4	4	4	6	46
Terminación en 9	5	5	3	4	6	3	2	4	4	2	38
Totales	25	21	16	16	17	14	16	14	15	14	168

	DECENAS CON TERMINACIÓN COMPLETA			
Decena	1	3	7	9
100	101	103	107	109
190	191	193	197	199
820	821	823	827	829

	SUMA DE NÚMEROS PRIMOS COMPRENDIDOS ENTRE 1 Y 1000							
	Terminaciones				Evolución			
C	1	3	7	9	Sn	%n	San	%San
99	215	291	272	275	1.053	1,38	1.053	1,38
199	755	745	892	775	3.167	4,16	4.220	5,54
299	1.255	1.295	761	737	4.048	5,32	8.268	10,86
399	642	1.422	2.072	1.476	5.612	7,37	13.880	18,23
499	2.205	1.339	1.411	2.694	7.649	10,05	21.529	28,28
599	1.633	2.182	2.268	1.677	7.760	10,19	29.289	38,48
699	3.225	3.265	2.548	1.278	10.316	13,55	39.605	52,03
799	2.213	2.249	3.068	2.936	10.466	13,75	50.071	65,78
899	2.513	3.422	3.448	3.336	12.719	16,71	62.790	82,49
999	3.814	1.936	5.732	1.848	13.330	17,51	76.120	100,00
Sn	18.470	18.146	22.472	17.032	76.120	100,00		
%n	24,26	23,84	29,52	22,38	100,00			

Nota: La suma total de los 168 primos es de 76.127, ya que en el cuadro no se incluyen los primos especiales 2 y 5.

3.3 La función $D(m)=p+r$ de descomposición de un número en suma de factores primos.

La función $D(m)=p+r\cdots con\ r,p\in \Pr imos$, tiene como objetivo la descomposición de m en suma de dos o más números primos, $D(m)=p+r$, a partir de Q, $Q\in \mathbb{Q}$, siendo $Q=\frac{p}{r}$ si $mcd(p,r)=1$.

Si $a,b,c,d...$ son divisores de m y si se toman en grupos de $\{a,b\}$, $\{a,b,c\}$, $\{a,b,c,d\}$ como raíces que satisfacen estructuras de ecuaciones cuadráticas, cúbicas, cuárticas, etc., mediante la aplicación de fracciones unitarias podemos determinar la composición de los coeficientes dependientes de la ecuación, de acuerdo con la Ley de Coeficientes de Descartes o el Teorema de Polinomios Simétricos de Newton. A su vez, estos mismos coeficientes nos facilitan la descomposición del número m en suma de dos o más números primos. El valor de $m, m\geqq 1$ y si es primo o compuesto, condicionará el desdoblamiento.

Si a y b son las raíces que satisfacen a $x^2-Bx+C=(x-a)(x-b)$ entonces, por la Ley de Coeficientes de Descartes (*LCD*)

$$x^2-(a+b)x+ab=0 \text{ donde } \begin{cases} x_1=a \\ x_2=b \end{cases}.$$

Aplicando fracciones unitarias

$$\frac{1}{a}+\frac{1}{b}=\frac{Q}{Q+1},$$

resulta:

$$Q=\frac{a+b}{ab-(a+b)}=\frac{Bx}{C-Bx}=\frac{p}{r}$$

y, por tanto:

$$D(m)=p+r$$

Si a, b y c son raíces que satisfacen a $x^3-Bx^2+Cx-D=(x-a)(x-b)(x-c)$ entonces, por la (*LCD*)

$$x^3-(a+b+c)x^2+(ab+ac+bc)x-abc=0 \text{ donde } \begin{cases} x_1=a \\ x_2=b. \\ x_3=c \end{cases}$$

Aplicando $\frac{1}{a}+\frac{1}{b}+\frac{1}{c}=\frac{Q}{Q+1}$, resulta:

$$Q=\frac{ab+ac+bc}{abc-(ab+ac+bc)}=\frac{Cx}{D-Cx}=\frac{p}{r}$$

y, por tanto:

$$D(m)=p+r$$

Para la ecuación cuartica, $x^4-Bx^3+Cx^2-Dx+E=(x-a)(x-b)(x-c)(x-d)$ si a,b,c,d son sus raíces,

$$x^4-(a+b+c+d)x^3+(ab+ac+ad+bc+bd+cd)x^2-(abc+abd+acd+bcd)x+abcd=0.$$

Si $\frac{1}{a}+\frac{1}{b}+\frac{1}{c}+\frac{1}{d}=\frac{Q}{Q+1}$

resulta para

$$Q=\frac{a(cd+b(c+d))+bcd}{abcd-(a(cd+b(c+d))+bcd)}=\frac{Dx}{E-Dx}=\frac{p}{r}$$

y, por tanto:

$$D(m)=p+r$$

Veamos algunos ejemplos:

3.1 Descomponer el número 42 en suma de primos.

Sea $m=42=2\cdot3\cdot7$. Si tomamos los divisores 6 y 7 como raíces de una cuadrática y aplicando sus inversos en una fracción unitaria, tenemos

$$\frac{1}{6}+\frac{1}{7}=\frac{Q}{Q+1},\ Q=\frac{6+7}{6\cdot 7-(6+7)}=\frac{13}{42-13}=\frac{13}{29}$$

y, como $mcd(13,29)=1$, $D(m)=13+29=42$.
Si $x^2+Bx+C=(x-a)(x-b)$ entonces, $x^2-(a+b)x+ab=0$ donde $x_1=a\ y\ x_2=b$. Aplicado al caso planteado, $x^2-13x+42=0$ donde $x_1=6$ y $x_2=7$.
Si tomamos los divisores $6,7\ y\ 7$ como raíces de una cúbica y aplicando sus inversos en una fracción unitaria, tenemos

$$\frac{1}{6}+\frac{1}{7}+\frac{1}{7}=\frac{Q}{Q+1},\ Q=\frac{6\cdot 7+6\cdot 7+7\cdot 7}{6\cdot 7\cdot 7-(133)}=\frac{133}{294-133}=\frac{133}{161}=\frac{19}{23}$$

ya que $mcd(133,161)=7$ y, por tanto $D(m)=19+23=42$.
Si $x^3+Bx^2+Cx+D=(x-a)(x-b)(x-c)$, como $x^3-(a+b+c)x^2+(ab+ac+bc)x-abc=0$, entonces $x_1=a, x_2=b\ y\ x_3=c$.
Aplicado al caso planteado, $x^3-20x^2+133x-294=0$, donde $x_1=6, x_2=7\ y\ x_3=7$.

3.2 Descomponer el número 420 en suma de primos.
Sea $m=420=2^2\cdot 3\cdot 5\cdot 7$. Si tomamos los divisores $3,4,5\ y\ 7$ como raíces de una cuartica y aplicando sus inversos en una fracción unitaria, tenemos

$$\frac{1}{3}+\frac{1}{4}+\frac{1}{5}+\frac{1}{7}=\frac{Q}{Q+1},\ Q=\frac{3(5\cdot 7+4(5+7))+4\cdot 5\cdot 7}{3\cdot 4\cdot 5\cdot 7-(389)}=\frac{389}{420-389}=\frac{389}{31}$$
$$D(m)=31+389=420.$$

Si $x^4-Bx^3+Cx^2-Dx+E=(x-a)(x-b)(x-c)(x-d)$ entonces,
$x^4-(a+b+c+d)x^3+(ab+ac+ad+bc+bd+cd)x^2-(abc+abd+acd+bcd)x+abcd=0$
que admite las raíces $x_1=a, x_2=b, x_3=c\ y\ x_4=d$. Aplicado al caso planteado, genera la ecuación $x^4-19x^3+131x^2-389x+420=0$ cuyas raíces son, $x_1=3, x_2=4, x_3=5\ y\ x_4=7$.

3.3 Descomponer el número 48 en suma de primos.
Sea $m=48=2^4\cdot 3$. Si tomamos 2 y 24, dos de sus divisores, obtenemos

$$\frac{1}{2}+\frac{1}{24}=\frac{Q}{Q+1}\Rightarrow Q=\frac{2+24}{2\cdot 24}=\frac{26}{48-26}=\frac{26}{22}=\frac{13}{11}.$$

$D(m)=11+13=24$, que es la mitad de m, por lo que podemos establecer

$$D(m)=11+11+13+13=24$$

pero no lo haremos.
Tomemos uno de los primos, por ejemplo el 13, y operemos con el resto, $48-13=35$.

$$\frac{1}{5}+\frac{1}{7}=\frac{Q}{Q+1}\Rightarrow Q=\frac{5+7}{5\cdot 24-12}=\frac{12}{35-12}=\frac{12}{23}.$$

Ahora $D(m)=13+23+12=48$, donde uno de los sumando no es primo. Operamos

$$\frac{1}{3}+\frac{1}{4}=\frac{Q}{Q+1}\Rightarrow Q=\frac{3+4}{3\cdot 4-7}=\frac{7}{12-7}=\frac{7}{5}$$

Finalmente:

$$D(m)=5+7+13+23=48.$$

Si el primo elegido hubiera sido el 11, $D(m)=11+37=48,$ sería otro desdoblamiento.

3.4 Descomponer el número 63 en suma de primos.

Se trata de un número impar a factorizar como $m=63=3^2\cdot 7.$ Tomemos el 7 y el 9 como divisores de 63

$$\frac{1}{7}+\frac{1}{9}=\frac{Q}{Q+1}\Rightarrow Q=\frac{7+9}{63-16}=\frac{16}{47}$$

$D(m)=16+47=63,$ pero 16 no es primo, $m=16=2^4$

$$\frac{1}{2}+\frac{1}{8}=\frac{Q}{Q+1}\Rightarrow Q=\frac{2+8}{16-10}=\frac{10}{6}=\frac{5}{3}$$

Podemos obtener, bien $D(m)=3+13+47=63$ o bien $D(m)=5+11+47=63.$

2. 4. *Clasificación de los números primos.*

4.1 Euclides y los números primos.

$Euclides\ de\ Alejandría\ (325-265)$ dice, en la proposición 20 del libro noveno de su obra *Los Elementos*, que *hay más números primos que cualquier cantidad propuesta de números primos*. La demostración de Euclides por reducción al absurdo, es como sigue:

> Supongamos que hubiera una lista sólo con un número finito de primos, $p_1,p_2,\ldots,p_n$; si el número $p_1,p_2,\ldots,p_{n+1},$ no es divisible por $p_1,p_2,\ldots,p_n$ o bien es primo, o bien debe haber algún otro primo que lo divida, no incluido en la lista luego, esa lista no incluye a todos los números primos, en contradicción con la hipótesis, y debe haber una cantidad infinita de primos.

Establecido que, dado un entero $p,\ p\in\mathbb{N},\ p>1,$ se dice que es un número **primo absoluto**, o simplemente **primo**, cuando no admite más divisores en $\mathbb{N}$ que el 1 y el propio $p.$ Por otra parte, para todo valor de $m\in\mathbb{N},$ la expresión m^2-m es un número compuesto. En efecto, como $m^2-m=m(m-1)$ es producto de dos números consecutivos, uno par y el otro impar, por tanto $2|(m^2-m)$ y, en consecuencia, m^2-m es un número compuesto.
Para estudiar la distribución de los primos en una cantidad dada, la función $\pi(x)$ cuenta el número de primos $\leqq x$ que verifica para $2\leqq p\leqq x,\ p\in primo.$ Esta función tiene como límite la unidad y se denota como $\lim_{\to\infty}\frac{\pi(x)}{x/\ln x}=1,$ ln (logaritmo natural).

4.2 Propiedades de los números primos.

Algunas de las propiedades de los números primos son:

Si *p* es un número primo y divisor del producto de números enteros $a \cdot b$, entonces p es divisor de *a* o de *b*. (Lema de Euclides).
Si *p* es primo y *a* es algún número natural diferente de 1, entonces $a^p - a$ es divisible por *p*. (Pequeño Teorema de Fermat).
Un número *p* es primo si y sólo si el factorial $(p-1)!+1$ es divisible por *p*. (Teorema de Wilson).
Si *n* es un número natural, entonces siempre existe un número primo *p* tal que $n < p < 2n$. (Postulado de Bertrand).
En toda progresión aritmética $a_n = a + nq$, donde los enteros positivos $a, q \geqq 1$ son primos entre sí, existen infinitos números primos. (Teorema de Dirichlet).
El número de primos menores que un x dado sigue una función asintótica a $f(x) = \frac{x}{\ln x}$. (Teorema de los números primos).
El anillo $\mathbb{Z}/n\mathbb{Z}$ es un cuerpo si y sólo si n es primo. Equivalentemente: n es primo si y sólo si $\varphi(n) = n-1$, donde $\varphi(n)$ es la función *fi* de Euler.

4.3 Números de Fermat.

Entre las muchas clasificaciones de números primos que existen, algunas de las principales, son:

Número primo de Fermat, de la forma $F_p = 2^{2^n} + 1$.

Se denominan *números de Fermat* en honor a $Pierre\ de\ Fermat\ (1601-1665)$, matemático francés y una de las figuras más destacadas del siglo XVII, junto a Descartes, Mersenne o Pascal. Fermat fue el primero en estudiar estos números y conjeturó que todos los números naturales de la forma $2^{2^n}+1$, $n \in \mathbb{N}$ eran números primos y, así es para $n = 0,1,2,3$ *y* 4, $F_0 = 2^1 + 1 = 3$, $F_1 = 2^2 + 1 = 5$, $F_2 = 2^4 + 1 = 17$, $F_3 = 2^8 + 1 = 257$ y $F_4 = 2^{16} + 1 = 65.537$. Sin embargo, para $F_5 = 2^{32} + 1 = 4.294.967.297 = 641 \cdot 6700417$, es el número más pequeño que, siendo número de Fermat, no es primo. Esta circunstancia fue probada en 1732 por Euler.
Podemos establecer las siguientes propiedades a los números de Fermat:
Un número de Fermat es igual al producto de todos los anteriores más 2. Esto se puede demostrar por inducción como sigue:
Si $n = 1$, es verdad: $F_1 = F_0 + 2 (5 = 3 + 2)$.
Si se cumple para *k* igual a $n-1$, se cumple para *n*:

$$\begin{aligned} F_0 \cdot F_1 \cdot \ldots \cdot F_{n-2} + 2 &= (F_{n-1} - 2)(F_{n-1} + 2) \\ &= (2^{2^{n-1}} + 1 - 2)(2^{2^{n-1}} + 1) + 2 \\ &= (2^{2^{n-1}} - 1)(2^{2^{n-1}} + 1) + 2 \\ &= (2^{2^{n-1}})^2 - 1 + 2) = 2^{2^n} + 1 = F_n \end{aligned}$$

La propiedad anterior nos permite deducir que:
Ningún número de Fermat puede ser suma de dos números primos. Como todos los números de Fermat son impares, uno de los sumandos debe ser 2. Entonces, el otro tendrá que ser, o bien 1 (caso de $F_0 = 3$) o bien el producto de todos los anteriores, pero precisamente por ser producto de números naturales, no puede ser primo.

Dos números de Fermat distintos siempre son primos entre sí, es decir, no tienen ningún factor común. Se sabe que $F_n = F_0 \cdot F_1 \cdot \ldots \cdot F_{n-1} + 2$. Como todos los números de Fermat son impares y por tanto 2 no puede ser un factor común, se concluye que F_n no es divisible por ninguno de los factores de los anteriores números de Fermat.

Todo número compuesto de Fermat $F_n = 2^{2^n} + 1$ se puede descomponer en factores primos de la forma $k \cdot 2^{2^n} + 1$, con *k* entero positivo.

4.4 Números de Mersenne.

Número primo de Mersenne, de la forma $M_p = 2^p + 1$.

Los números de Mersenne deben su denominación a $Marin\ Mersenne\ (1588 - 1648)$, monje francés, filósofo y matemático que se constituyó en canal de comunicación entre sus coetáneos Descartes, Fermat, Galileo y Pascual. Se dice que un número M es un *número de Mersenne* si es una unidad menor que una potencia de 2, $M_p = 2^p + 1$.

A fecha de septiembre de 2008, sólo se conocen 46 números primos de Mersenne, siendo el mayor de ellos $M_{46} = 2^{43112609} - 1$. Algunos de estos números son,

> 3, 7, 31, 127, 8191, 131071, 524287, 2147483647, 2305843009213693951, 618970019642690137449562111, 162259276829213363391578010288127, 170141183460469231731687303715884105727.

Otros números de Mersenne, pueden ser,

> 2, 3, 5, 7, 13, 17, 19, 31, 61, 89, 107, 127, 521, 607, 1279, 2203, 2281, 3217, 4253, 4423, 9689, 9941, 11213, 19937, 21701, 23209, 44497, 86243, 110503, 132049, 216091, 756839, 859433, 1257787, 1398269, 2976221, 3021377, 6972593, 13466917.

Las propiedades de los números de Mersenne se pueden resumir:

> Si *n* es compuesto, entonces M_n es compuesto.
>
> Si *p* es un número primo distinto de 2, cualquier primo *q* que divida a $2^p - 1$ debe ser uno más que un múltiplo de $2p$. Esta proposición también se cumple si $2^p - 1$ es primo.
>
> Si *p* es un número primo distinto de 2, cualquier primo *q* que divida a $2^p - 1$ es congruente con $\pm$ (*mód*.8). Como $2^{p+1} \equiv 2(mód.q)$, donde $2^{(p+1)/2}$ es una raíz cuadrada de $2\ módulo\ q$, por reciprocidad cuadrática, cualquier módulo primo del cual 2 tenga raíz cuadrada, es congruente con $\pm$ (*mód*.8).

Un número doble de Mersenne se define como $M_{Mp} = 2^{2^{p-1}} - 1$, donde p es el exponente de un número primo de Mersenne.

4.5 Números de Sophie Germain.

Un número primo p es un número de Sophie Germain si $2p+1$ también es número primo. Por ejemplo, $p = 2 \cdot 5 + 1 = 11$, $P = 2 \cdot 11 + 1 = 23$ donde 23 es un número primo de Germain. Los números primos de Germain reciben su nombre de $Sophie\ Germain\ (1776 - 1831)$, una matemática francesa que hizo importantes contribuciones a la teoría de los números y a la teoría de la elasticidad. Demostró que el Último Teorema de Fermat era cierto para estos números,

esto es, que si p es un número primo de estas características entonces, no existen soluciones enteras no triviales para la ecuación $x^p + y^p = z^p$.
Se conjetura que existen infinitos números primos de Sophie Germain, pero, al igual que la conjetura de los números primos gemelos, aún no se ha demostrado.
La secuencia $\{p, 2p+1, 2(2p+1)+1, \ldots\}$ de primos de Sophie Germain, también recibe el nombre de cadenas de Cunninghan, en honor a $Allan\ J.C.Cunninghan\ (1842-1928)$, militar de la Armada Británica, que las descubrió. Algunas de estas cadenas las podemos encontrar en la obra de *Thomas Koshy, Elementary Number Theory with Applications*, como:

2-5-11-23-47, 89-179-359-719-1439-2879, entre otras.

De la obra de Thomas W. Cusick y otros, *Stream Ciphers and Number Theory*, tomamos la siguiente propiedad para confeccionar tablas de números primos de Sophie Germain.
Si $p\ y\ q$ son dos números primos de Germain, si $p \equiv 1(mód.4)\ y\ q \equiv 3(mód.4)$ satisfacen a $p = 2p_1 + 1\ y\ q = 2p+1 = 4(p_1+1)-1$ entonces, se pueden confeccionar listas de números primos de la forma $2p+1$, como,

2,3,5,11,23,29,41,53,83,89,113,131,173,179,191,233,239,251,281,293,359,419,431,443,491,509

O bien, de la forma $(p-1)/2$,

5,7,11,23,47,59,83,107,167,179,227,263,347,359,383,467,479,503

4.6 Otros números primos.

Entre otros, podemos citar a:
Números primos de Wagstaff, en honor al matemático Samuel S.Wagstaff Jr, que son de la forma $p = (2^n+1)/3,\ p, n \in$ *primos de Mersenne*. Por ejemplo, 11, 43, 683, 2731, 43691,174763.
Números de Wagstaff, que son de la forma $p = (2^q+1)/3$, y que pueden ser primos o probablemente primos, como

$$3,11,43,683,2731,43691,174763,2796203,715827883,2932031007403$$

Números de Wieferich, en honor a $Arthur\ J.A.Wieferich\ (1884-1954)$, que en 1909 los describió en sus trabajos sobre el *Último Teorema de Fermat*. Son de la forma $p = p^2/(2^{p-1}-1)$. Los únicos números primos de Wieferich conocidos son el 1093 y 3511, si existen otros, deben ser mayores que 1, 10^{15}. Aunque se ha conjeturado que sólo existen un número finito de números primos de Wieferich, en 1988 J.H Silverman demostró que si la conjetura *abc* es válida, para todo número entero positivo $a > 1$, existen infinitos números primos *p* tal que p^2 no divide a $(a^{p-1}-1)$.
Un número de Wolstenholme, que reciben su nombre en honor a Joseph Wolstenholme (1829-1891), es un número primo *p* si cumple la condición de $\binom{2p \quad -1}{p \quad -1} \equiv (mód.p^4)$. Los únicos primos de Wolstenholme que se conocen son el 16843 y el 2.124.679. Cualquier otro primo será superior a 10^9, como demostró Charles Baddage en 1862.

Los numeradores de las sumas de los *números armónicos*, tales como, $\sum_{t=1}^{n} 1/t$ ó $\sum_{t=1}^{n} 1/t^k$ generan infinitos primos y posibles primos de Wolstenholme. Por ejemplo para $t\ y\ t^3$ tenemos:

1,3,11,25,137,49,363,761,7129,7381,83711,86021,1145993,1171733,1195757
1,9, 251, 2035, 256103, 28567, 9822481, 78708473, 19148110939,19164113947

Se dice que un número p es de Wilson cuando p^2 divide a $(p-1)!+1$, donde "!" denota la función factorial. Los únicos primos conocidos de Wilson son el 5, 13 y 563, generados mediante la forma $(p-1)!\equiv -1(mód.p^2)$. De existir algún otro, sería superior a $5\cdot 10^8$.
Por el teorema de Wilson-Lagrange resulta que un entero p, $p>1$ y primo, será primo si, y sólo si, $(p-1)!\equiv -1(mód.p)$.
Números de la forma $3n-1$ conocidos como primos de Eisenstein, en honor a Ferdinand G. Eisenstein (1823-1852), son primos ordinarios con $p\equiv 2(mód.3)$, es decir:

2,5,11,17,23,29,41,47,53,59,71,83,89,101,107,113,131,137,149,167,
173,179,191,197,227,233,239,251,257,263,269,281,293, 311,317,347

Se conocen como enteros de Gauss, en honor a Carl Friedrich Gauss (1777-1855), a aquellos números que tienen la forma $n=4k+1$ y son susceptibles de ser representados como suma de dos cuadrados. Entre ellos podemos encontrar:

5,9,13,17,21,25,29,33,37,41,45,49,53,57,61,65,69,73,77,81,85,89,93,97,
101,105,109,113,117,121,125,129,133,137,141,145,149,153,157,161,
165,169, 173,177,181,185,189,193,197,201, 205,209,213,217,221,225.

Se conocen como primos de Gauss a aquellos primos de la forma $n=4k+3$ que son irreducibles en la factorización única de dominios integrales. Por ejemplo:

5,11,17,23,31,41,47,59,67,73,83,97,103,109,127,137,149,157,167,179,
191,197,211,227,233,241,257,269,277,283,307,313,331,347,353,367,
379,389,401,419,431,439,449,461,467,487,499,509,523,547,563,571.

4.7 Números gemelos.

Dos números primos p,q son gemelos si están separados por una distancia de 2, es decir, p y $p+2$ donde $q=p+2$. No se sabe si existen infinitos números primos gemelos, aunque se cree ampliamente que sí. Hardy y Littlewood conjeturaron una ley de distribución de los números primos gemelos similar al teorema de los números primos. Se ha demostrado que el par p y $p+2$ es de números primos gemelos si, y sólo si, $4((p-1)!+1\equiv -p(mód.p(p+2))$.
Una representación de estos números la podemos ver a continuación:

{3,5},{5,7},{11,13},{17,19},{29,31},{41,43},{59,61},{71,73},{101,103},{107,109},{137,139},{149,151}
{179,181},{191,193},{197,199},{227,229},{239,241},{269,271},{281,283},{311,313},{347,349},
{419,421},{431,433},{461,463},{521,523},{569,571},{599,601},{617,619},{641,643},{659,661},
{809,811},{821,823},{827,829},{857,859},{881,883},{1019,1021},{1031,1033},{1049,1051},
{1061,1063},{1091,1093},{1151,1153}

2. 5. *Temas de discusión.*

5.1 Si r es el residuo cuando 1059, 1417 y 2312 se divide por $d>1,$ determinar el valor de $d-r.$

Por el Algoritmo de Euclides, hay enteros q_1, q_2, q_3 donde $1059 = dq_1 + r,$ $1417 = dq_2 + r$ y $2312 = dq_3 + r.$ Sacando diferencias obtenemos:

$$1253 = d(q_3 - q_1),\ 895 = d(q_3 - q_2) \text{ y } 358 = d(q_2 - q_1)$$

Como el $mcd(1253, 895, 358) = 179,$ resulta para $d = 179.$
Como $1059 = 5 \cdot 179 + 164,$ resulta para $r = 164,$ luego

$$d - r = 179 - 164 = 15$$

Nota: Problema de AHSME (*American High School Mathematics Examination*) de 1976.

5.2 Demuestra que $n^2 + 23$ es divisible por 24 para un número infinito de números $n.$

Si tenemos en cuenta que

$$n^2 + 23 = n^2 - 1 + 24 = (n-1)(n+1) + 24$$

entonces, las familias

$$n = 24m \pm 1,\ \ m = 0,\ \pm 1,\ \pm 2,\ \pm 3, \ldots$$

producen infinitos valores de la forma $n^2 + 23$ que son divisibles por 24.

5.3 Demuestra que existe un entero único n para el cual $2^8 + 2^{11} + 2^n$ es un cuadrado perfecto.

Sea $k^2 = 2^8 + 2^{11} + 2^n = 2304 + 2^n = 48^2 + 2^n,$ entonces $k^2 - 48^2 = (k-48)(k+48) = 2^n.$
Si $k - 48 = 2^s,$ $k + 48 = 2^t$ y $s + t = n,$ resulta que $2^t - 2^s = 96 = 3 \cdot 2^5$ o $2^s(2^{t-s} - 1) = 3 \cdot 2^5$ luego, $s = 5$ y $t - s = 2,$ por lo que $s + t = n = 12.$
La solución resulta

$$2^8 + 2^{11} + 2^{12} = 80^2$$

5.4 Encontrar el cuadrado perfecto más pequeño que es divisible por 7!.

El factorial de 7! es igual a $7! = 7 \cdot 6 \cdot 5 \cdot 4 \cdot 3 \cdot 2 \cdot 1 = 5040 = 7 \cdot 5 \cdot 3^2 \cdot 2^4.$ Un número es cuadrado perfecto si y sólo si todos los exponentes de su factorización son pares. Un cuadrado perfecto que sea divisible por 7! y sea el menor posible es

$$n = 7^2 \cdot 5^2 \cdot 3^2 \cdot 2^4 = 7 \cdot 5 \cdot (7 \cdot 5 \cdot 3^2 \cdot 2^4) = 176400 = 420^2$$

5.5 Hallar dos números que sumen 240 y que su mcm sea 1768.

Sea $a+b=D(q+q')$ y sea $a=Dq$ y $b=Dq'$ donde $DM=Dq\cdot Dq'=D(q\cdot q')$, resulta $M=D(q\cdot q')$.
Si ahora dividimos miembro a miembro

$$\frac{a+b}{M}=\frac{D(q+q')}{Dq\cdot q'}=\frac{q+q'}{q\cdot q'}$$

esto es

$$\frac{a+b}{M}=\frac{q+q'}{q\cdot q'}$$

luego

$$\frac{240}{1768}=\frac{q+q'}{q\cdot q'}=\frac{30}{221}$$

de donde $q+q'=30$ y $q\cdot q'=221$, haciendo que $q'=30-q$, $q(30-q)=221$, $30q-q^2=221$, y teniendo en cuenta que $q^2-30q+221=0$, resolvemos

$$q=\frac{30\pm\sqrt{900-884}}{2}=\frac{30\pm 4}{2}=\begin{cases}x_1=17\\x_2=13\end{cases}$$

luego, las soluciones del sistema son: para $q=17$ y para $q'=13$, y para $q=13$ y para $q'=17$. Teniendo en cuenta $q\cdot q'$, podemos calcular los números pedidos *a* y *b*, previo cálculo del mcd. Como $D=\frac{M}{q\cdot q'}=\frac{1768}{17\cdot 13}=8$ tenemos

$$\begin{cases}a=Dq=8\cdot 17=136\\b=Dq'=8\cdot 13=104\end{cases}$$

por tanto, los números pedidos son el 136 y el 104.

5.6 Hallar dos números cuyo producto sea 10800 y su mcd 60.

Sea $a\cdot b=Dq\cdot Dq'=D^2qq'$ esto es $a\cdot b=D^2qq'$.
Si tenemos en cuenta que $\frac{a\cdot b}{D^2}=\frac{D\cdot M}{D^2}=qq'=\frac{M}{D}$ entonces, $M=Dqq'$.
Para el supuesto planteado

$$qq'=\frac{a.b}{D^2}=\frac{10800}{60^2}=3\rightarrow\begin{cases}q=3\\q'=1\end{cases}$$

de donde, los números pedidos serán

$$\left.\begin{array}{l} a = dq \;\; = 60.3 = 180 \\ b = dq' = 60.1 = \;\; 60 \end{array}\right\} = 180 \cdot 60 = 10800.$$

Otra solución habría sido $mcm = a \cdot b / mcd = 10800 / 60 = 180.$

5.7 Hallar dos números cuyo cociente sea 33/21 y su mcd 90.

Sea $\frac{a}{b} = \frac{Dq}{Dq'} = \frac{q}{q'} \rightarrow aq' = bq.$ Si $\frac{a}{b} = \frac{q}{q'} = \frac{33}{21} = \frac{11}{7}$

de donde $q = 11$ y $q' = 7$

resulta

$$\begin{cases} q = Dq = 90 \cdot 11 = 990 \\ q' = Dq' = 90 \cdot 7 = 630 \end{cases}$$

que son los números solicitados.

BIBLIOGRAFIA:

ALLENBY, R.B.J.T., Rings, Fields and Groups, ISBN: 0-340-54440-6
APOSTOL, Tom M. Introducción a la Teoría Analítica de Números, ISBN: 84-291-5006-4
AYRES, Frank Jr., Álgebra Moderna, ISBN: 968-422-917-8
BIRKHOFF, G. y MAC LANE, S., Álgebra Moderna, ISBN: 84-316-1226-6
CUSICK, Thomas y otros, Stream Ciphers and Number Theory, ISBN: 0-444-51631-X
KOSHY, Thomas, Elementary Number Theory with Aplications, ISBN: 978-0-12-372487-8
TATTERSALL, James J., Elementary Number Theory in Nine Chapters, ISBN: 0-521-61524-0
VINOGRADOV, Iván M. Fundamentos de la Teoría de los Números, Editorial Mir-Moscú

APOYO INTERNET:

http://es.wikipedia.org/wiki/Divisibilidad
http://es.wikipedia.org/wiki/M%C3%A1ximo_com%C3%BAn_divisor
http://es.wikipedia.org/wiki/M%C3%A9todo_de_factorizaci%C3%B3n_de_Euler
http://es.wikipedia.org/wiki/M%C3%A9todo_de_factorizaci%C3%B3n_de_Fermat
http://es.wikipedia.org/wiki/N%C3%BAmeros_primos_gemelos
http://mathworld.wolfram.com/
http://wims.unice.fr/wims/wims.cgi?lang=es&+session=ST4505DC81.1 (Programa matemático)
http://wmatem.eis.uva.es/~matpag/INICIALES/marco_principal.htm
http://www.btinternet.com/~se16/js/factor.htm#Top (Calculadora de factorización)
http://www.cidse.itcr.ac.cr/revistamate/contribuciones-v6-n1-set2005/factorizacion/factorizacion.pdf
http://www.hojamat.es/
http://www.newsgrupos.com/archive/f-29.html
http://www.positiveintegers.org/
http://www.wolframalpha.com/examples/ (Programa matemático)