Aritmética

Introducción

Bautizo: Decimos **a** ***divide*** a **b** (**a** ***factor*** de **b**, **a** es ***divisor*** de **b**, **b** es ***múltiplo*** de **a**, **b** es ***divisible*** por **a**) si existe un entero **c** tal que **b=ac**. Lo anterior se simboliza como **a|b**, en caso de que **a** no divida a **b**, se simbolizará como **a ∤ b**.

De la definición anterior se pueden deducir las siguientes propiedades:

Si **a|b** y **a|c** entonces **a|b+c**
Si **a|b** entonces **a|bc**
Si **a|b** y **a|b+c** entonces **a|c**
(Propiedad reflexiva) **a|a**
(Propiedad Transitiva) Si **a|b** y **b|c** entonces **a|c**

P1: ¿Cuándo se cumple la Simetría? **a|b** y **b|a**

Observación: Es conveniente hacer notar que el símbolo | NO es el símbolo de división, sino un símbolo de relación, así pues, aunque la división $\frac{0}{0}$ no está definida, podemos decir que $0 \mid 0$, ya que existe un entero (de hecho, cualquier entero) que cumple que $0c=0$.

A2: (G1) Encuentra los valores de a, tales que **0|a**
A3: (G1) Encuentra los valores de a, tales que **a|0**
A4: (G1) ¿Para que valores de n se cumple que $n-2 \mid n+2$?
A5: (G1) ¿Para que valores de n se cumple que $n-2 \mid n^2-3$?
A6: (G1) ¿Para que valores de n se cumple que $3 \mid n^2-2$?
A7: (G1) ¿Para que valores de n se cumple que $n-2 \mid 2n$?
A8: (G1) Prueba que 1 sumado al producto de cuatro enteros consecutivos es un cuadrado.
A9: (G1) Prueba que 1 sumado al producto de dos enteros impares consecutivos o de dos enteros pares consecutivos es un cuadrado.
A10: (G1) Prueba que el producto de cuatro enteros positivos consecutivos no puede ser un cuadrado.

A11: (G1) Prueba que para todo entero no negativo n, $(3+\sqrt{5})^n+(3-\sqrt{5})^n$ es entero un divisible por 2^n.

A12: (G1) Si a y b son enteros positivos, calcula a y b si $(a+b)^2=2304$ y $a^2+b^2=1250$.

A13: (G1) Si a es un entero impar. Probar que a^2-1 es divisible por 8.

A14: (G1) Si a es un entero impar. Probar que a^4-1 es divisible por 16.

A15: (G1) Si a es un entero impar. Probar que $a^{2^n}-1$ es divisible por 2^{n+2}.

Para los ejercicios A4 al A14, se sugiere usar Inducción Matemática.

A16: (G1) Demuestra que $3 \mid 4^n-1$

A17: (G1) Demuestra que $11 \mid 3^{2n+2}+2^{6n+1}$

A18: (G1) Demuestra que $17 \mid 3^{4n+2}+2\cdot 4^{3n+1}$

A19: (G1) Demuestra que $11 \mid 2^{2n-1}\cdot 3^{n+2}+1$

A20: (G1) Demuestra que $64 \mid 3^{2n+2}-8n-9$

A21: (G1) Demuestra que $11 \mid 5^{5n+1}+4^{5n+2}+3^{5n}$

A22: (G1) Demuestra que $288 \mid 7^{2n+1}-48n-7$

A23: (G1) Demuestra que $17 \mid 3\cdot 5^{2n+1}+2^{3n+1}$

Para los siguientes ejercicios puedes suponer que el coeficiente binomial es entero, $\binom{n}{k}=\frac{n!}{k!(n-k)!}$.

A24: (G1) Sean m, $a_1,a_2,\ldots,a_n$ enteros positivos tales que $a_1+a_2+\ldots+a_n=m$, prueba que $\frac{m!}{a_1!a_2!\ldots a_n!}$ es un entero no negativo.

A25: (G1) Prueba que $(n!)^2$ divide a $(2n)!$, y que $\frac{(2n)!}{(n!)^2}$ es par.

A26: (G1) Prueba si dos números son suma de dos cuadrados, entonces su producto es también la suma de dos cuadrados.

A27: (G1) Sea $f:N\to N$ la aplicación definida por $f(n)=\frac{n}{2}$ si n es par, $f(n)=3n+1$ si n es de la forma $n=4k+1$ y $f(n)=3n-1$ si n es de la forma $n=4k+3$. Probar que para todo $n\in N$ existe $i\in N$ tal que $f^i(n)=1$. ($f^i(n)$ significa la composición de f^i en sí misma i veces.

A28: (G1) Sea $f: N \to N$ la aplicación definida por $f(n) = \frac{n}{3}$ si n es divisible por tres, $f(n) = 2n+1$ si n es de la forma $n = 3k+1$ y $f(n) = 2n-1$ si n es de la forma $n = 3k+2$. Probar que para todo $n \in N$ existe $i \in N$ tal que $f^i(n) = 1$.

Chisme: Algoritmo de Siracusa
Sea $f: N \to N$ la aplicación definida por $f(n) = \frac{n}{2}$ si n es par, y $f(n) = 3n+1$ si n es impar. Probar que para todo $n \in N$ existe $i \in N$ tal que $f^i(n) = 1$.
Este algoritmo también es conocido como: Problema $3x+1$, Algoritmo de Hasse, Problema de Kakutani, Problema de Siracusa, Conjetura de Thwaites, Problema de Ulam.
Thwaites en 1996 ofreció una recompensa de £1000 a quien lo resolviera. Hasta el momento se ha probado sólo para los números naturales n tales que $n \leq 3 \cdot 2^{53}$.

A29: (G1) Prueba que $(2m)! \cdot (2n)!$ es divisible por $(n)! \cdot (m)! \cdot (m+n)!$.

Números Primos

Bautizo:
Un número entero es **primo** si y solamente si tiene cuatro diferentes divisores.

Observaciones: El 1 y el -1 tienen sólo dos divisores (el 1 y el -1), por lo cual no son primos. Por otra parte, cualquier número divide al cero, por lo cual tiene más de 4 divisores, entonces no es primo. Los divisores *triviales* de un número n son 1, -1, n y $-n$. Como cualquier número diferente del 1 y -1, tiene al menos 4 divisores (los *triviales*), un número no es primo si tiene un divisor no *trivial*.
Tres bautizos:
A los números 1 y -1 se les llama **unidades**.
Un número entero, que no es unidad y no es primo se llama **compuesto**.
Dos números a y b son **coprimos** o **primos entre sí** o **primos relativos** si satisfacen que $d|a$ y $d|b \Rightarrow d = 1$ o $d = -1$.

Proposición: Si a, b y c son números naturales diferentes de cero, entonces $a = b \cdot c$ implica que $a \leq b$ y $a \leq c$. (Sugerencia: $1 \leq b$ y $1 \leq c$).

Proposición: Si $a \in \mathbb{Z} - \{-1, 0, 1\}$ y a no es un número primo existe, b, tal que $1 < b < |a|$ y $b | a$.

Proposición: Todo entero distinto de 1 y -1 es divisible por un número primo. (Sugerencia: ¿Qué pasaría si no fuera cierto?).

Proposición: Hay una cantidad infinita de primos. (Sugerencia: Si no fuera cierto, ¿es un número primo la suma de 1 con el producto de todos los primos?)

B1: (G1) Todo primo de la forma $3k+1$ es de la forma 6k+1.
B2: (G1) Prueba que hay una infinidad de primos de la forma $4k+3$ y $6k+5$.
B3: (G1) Prueba que hay una infinidad de primos de la forma $4k+1$.

Teorema de Dirichlet: Si a y b son primos relativos entonces hay una cantidad infinita de primos de la forma $ak+b$. (La demostración de este teorema la puedes encontrar en http://paraisomat.ii.uned.es/archivos/tnumeros/ap_dirichlet.zip).

Chisme: El Teorema de Dirichlet fue conjeturado por Gauss (considerado por varios como el matemático más grande de historia) y demostrado por Dirichlet en 1837. Johann Peter Gustav Lejeune Dirichlet nació en Düren, Alemania, en 1833 y murió el año de 1877 en Gotinga, Alemania. Su nombre, Lejeune Dirichlet, deriva de que su familia era de Richlet, una población de Bélgica, y Lejeune Dirichlet $\approx$ "le jeune de Richelet" = "el joven de Richelet". Sus principales aportaciones fue en el área de Teoría de Números. Si primera publicación trató sobre el Teorema de Fermat, donde demostró su veracidad para $n = 5$, tiempo después lo demostró para $n = 14$. Chisme de lavadero: Se caso con la hermana de Félix Mendelssohn, el autor de la célebre Marcha Nupcial.

B4: (G1) Prueba que 3, 5 y 7 es la única terna de primos positivos impares consecutivos.

B5: (G1) Si p_n es el n-ésimo primo. Prueba que ninguno de los números $p_1 \cdot p_2 \cdot \ldots p_n + 1$ es un cuadrado perfecto.
B6: (G1) Probar que para todo n existen n enteros consecutivos compuestos. (Sugerencia: ¿Qué pasaría si el primero de estos número fuera $(n+1)!+2$?)
B7: (G1) Prueba que no existe ningún polinomio $f(x) = a_n x^n + a_{n-1} x^{n-1} + \ldots + a_1 x + a_0$ con coeficientes enteros a_i y $n \geq 1$, tal que $f(m)$ sea primo para toda m.
B8: (G1) Si $2^n - 1$ es primo entonces n es 2 o n es impar.
B9: (G1) Si $2^n - 1$ es primo entonces n es primo.
B10: (G1) Si $2^n + 1$ es primo entonces n es potencia de 2.

Bautizos:
El número $F_n = 2^{2^n} + 1$ se llama **número de Fermat de orden n**.
Si $F_n = 2^{2^n} + 1$ es primo se dice que es un **Primo de Fermat**

B11: Probar que si $n \neq m$, entonces F_n y F_m son primos relativos.

B12: Probar inductivamente que si p_n es el n-simo primo, entonces $p_n \leq 2^{2^{2n-1}}$

Postulado de Bertrand: Si n>1, entonces existe siempre un primo p que satisface $n < p < 2n$.

B13: Usar el Postulado de Bertrand para probar que $p_n < 2^n, n > 1$, donde p_n es el n-simo primo.

Chisme: Joseph Louis François Bertrand (1800-1900) fue un profesor nacido en París. La conjetura la realizó en 1845, comprobando el resultado para cada entero n entre 2 y 6,000,000.
El resultado fue demostrado por primera vez por el matemático ruso P.L. Chebychev en 1850. Una demostración de Paul Ërdos, uno de los más grandes matemáticos del siglo XX, la cual descubrió a los 18 años la puedes encontrar en http://usuarios.lycos.es/teoriadenumeros/bertrand.html.

(B14) Probar que todo entero de la forma $4m+3$ tiene un número impar de factores de la forma $4m-1$.

(B15) Probar que si t es un entero mayor que uno, el número $t^{4m}+t^{2m}+1$ nunca es primo

(B16) Probar que el cubo de todo número entero es la diferencia de dos cuadrados enteros. (Sugerencia: $\left[\frac{n(n+1)}{2}\right]^2 = 1^3+2^3+\ldots+n^3$).

Algoritmo de la División

Teorema: Si a y b son enteros, $b \neq 0$, entonces existen dos enteros q y r, únicos, tales que $a = bq + r$, $0 \leq r < |b|$.

(C1) El resto de la división de un número al dividirlo por 4 es 3 y el resto de la división del mismo número al dividirlo por 9 es 5. Encontrar el resto de la división del mismo número entre 36.

Bautizos:

Denotaremos por $r_b(m)$ el resto de la de m por b.

(C2) $r_b(m+n) = r_b(r_b(m)+r_b(n))$

(C3) $r_b(m \cdot n) = r_b(r_b(m) \cdot r_b(n))$

(C4) Demuestra que un número es divisible por 9 si y sólo si la suma de sus dígitos en divisible por 9.

(C5) Demuestra que si la suma de los dígitos de un número n es s, entonces $r_9(n) = r_9(s)$.

(C6) Calcula el resto de la división de $(342109876543456643213 4567)^2$ entre 9.

(C7) Sean m y n enteros. Demuestra que si $7 | m^3+n^3+p^3$ entonces $7 | mnp$.

(C8) Sean m y n enteros. Demuestra que si $7 | \sum_{i=1}^{n} a^6$ entonces $7 | \prod_{i=1}^{n} a_i$ o $7 | n$.

(C9) Sean m y n enteros. Demuestra que si $7 | m^2+n^2$ entonces $7 | m$ y $7 | n$.

(C10) Sean m y n enteros. Demuestra que si $7 | m^4+n^4$ entonces $7 | m$ y $7 | n$.

(C11) Sean m y n enteros. Demuestra que si $7 | m^2+2n^2$ entonces $7 | m$ y $7 | n$.

(C12) Sean m y n enteros. Demuestra que si $7|m^2+4n^2$ entonces $7|m$ y $7|n$.
(C13) Sean a y b enteros, $b\neq 0$. Si $a-b=175$ y la división de a por b tiene cociente 15 y resto 7, hallar a y b.
(C14) Sean a y b enteros. Entonces a^3-b^3 es divisible por 11 si, y sólo si, $a-b$ es divisible por 11.
(C15) Dada una sucesión $a_1,a_2,...,a_n$ de enteros, probar que siempre es posible extraer una subsucesión cuya suma es divisible por n. (Sugerencia los n números $a_1,a_1+a_2,...,a_1+a_2+...+a_n$ y analiza sus restos).
(C16) Sea A un número escrito en forma decimal, forma los números $A_1=A,A_2=AA,A_3=AAA,...$ repitiendo las cifras de A. Demuestra que si m es un entero coprimo con 10, entonces m divide a una infinidad de números A_n.
(C17) Sean a,b y c enteros tales que $a^2+b^2=c^2$. Prueba que:
a) a o b es par.
b) a o b es divisible por 3.
c) a o b o c es divisible por 5.
d) a o b es divisible por 4.
e) Hallar todas las ternas coprimas $a,b,c\in N$, tales que $a^2+b^2=c^2$. (Respuesta: $a=x^2-y^2$, $b=2xy$, $c=x^2+y^2$, donde x e y recorren todos los enteros que satisfacen: $0<y<x$, $(x,y)=1$, x e y son de distinta paridad.
(C18) Probar que ningún entro positivo de la forma $8k+7$ puede expresarse como la suma de tres cuadrados enteros-
(C19) Sean p y q primos distintos, ambos mayores a tres. Probar que si $p-q$ es una potencia de 2, entonces p+q es divisible por 3.

Bautizo:
El máximo común divisor de dos números a y b, (a,b) o mcd(a,b), se define como el máximo entero con la propiedad de que divide a a y divide a b.
(C20) Si $d|a$, $d|b$ y existen u y v tales que $d=ua+vb$ entonces d=(a,b).
(C21) Si a,b,c,d y k son enteros. Demuestra que:
a) $(a,b,)=d\Rightarrow\left(\frac{a}{d},\frac{b}{d}\right)=1,d\neq 0$
b) $(a,b)=d\Rightarrow(ka,kb)=|k|d$

c) $(a,b+ka)=(a,b)$
d) $(a,b)=d$ y $(c,b)=1 \Rightarrow (ac,b)=d$

Teoremón: Si $(a,b)=d$, entonces existen enteros u y v tales que $(a,b)=ua+vb$.

(C22) $(a,b)=1$, $a|c$ y $b|c$ implica $ab|c$.
(C23) $(a,b)=1$, $a|bc$ implica $a|c$.
(C24) $\binom{2n}{n}$ es divisible por n+1.
(C25) Si a es primo entonces $240|a^4-1$.
(C27) Sean a y b enteros primos relativos. Calcula todos los valores posibles de $m=(3a-b,2a+b)$. (Resultado 5)
(C28) Sean a y b enteros primos relativos. Calcula todos los valores posibles de $m=(2a-5b,4a+3b)$. (Resultado 1, 2, 13, 26)
(C29) Hallar todos los enteros m tales que $13|(15m+14)^{18}$ (Resultado $\left\{\frac{13i+1}{2} | i\in \mathbb{Z} \text{ impar}\right\}$.
(C30) Si p es un número primo mayor a 3, entonces $p^2=24m+1$ para algún entero m. (Sugerencia: $p=3k+r$)

Bautizo: $m=[a,b]$ es el Mínimo común Múltiplo de los enteros a y b, si y sólo si cumple las dos condiciones:
1) m es múltiplo de a y b.
2) Si k es múltiplo de a y b entonces $m\le|k|$.

(C31) Si $a\in\mathbb{Z}$, entones $[a,a]=...$
(C32) Si $a,b\in\mathbb{Z}$, entones $[a,b]=b$ si, y sólo si …
(C33) $(a,b)=[a,b]$ si, y sólo si …
(C34) $[a,a]=|ab|$ si, y sólo si …
(C35) Demuestra que $[[a,b],c]=[a,[b,c]]$
(C36) $c>0$ implica $[ac,bc]=[a,b]c$
(C37) Si $d>0$, $d|a$ y $d|b$ entonces $\left[\frac{a}{d},\frac{b}{d}\right]=\frac{[a,b]}{d}$

(C38) Si $a|k$ y $b|k$, $a \neq 0 \neq b$ implica que $[a,b]|k$

(C39) Sea $m = \frac{|ab|}{(a,b)}$.

a) $[a,b]|m$

b) $m|[a,b]$ (Sugerencia: (a,b) es una combinación lineal de a y b).

c) $[a,b](a,b) = ab$

FO5-13) Si m y n son enteros positivos con $(n,m) = 1$, demuestra que $\frac{(m+n-1)!}{m!n!}$ es entero. (Sugerencia: $\binom{m+n-1}{m-1}$ y $\binom{m+n-1}{n-1}$ son enteros)

Lla) Expresa el máximo común divisor de cómo combinación lineal:

i) 228 y 348

ii) 15 y 21

iii) 2n+1, 4n

iv) $4n^2$+2n-40, 2n+7.

Súper Proposición: Una condición necesaria y suficiente para que la ecuación $ax + by = c$, a,b,c enteros, tenga solución en enteros, es que el máximo común divisor de a y b divida a c.

Otra súper proposición: El conjunto de soluciones enteras x, y de la ecuación $ax + by = c$, a,b,c enteros, es de la forma $x = x_0 + u;\ y = y_0 + v$ en donde x_0, y_0 es una solución particular de la ecuación $ax + by = c$, y u, v son solución de las ecuación homogénea asociada $ax + by = 0$

Otra más: Sean a,b y c enteros tales que a y b no son ambos ceros, supongamos además que $d = (a,b)$ divide a c. Sea $a = da'$, $b = db'$. Entonces el conjunto x, y de soluciones enteras de la ecuación $ax + by = c$ es $x = x_0 - b't$, $y = y_0 + a't$ donde t es un entero arbitrario y x_0, y_0 es una solución particular de la ecuación $ax + by = c$.

Llb) Encuentra todas las soluciones enteras de las siguientes ecuaciones diofantinas:

a) $15x + 21y = 300$

b) $228x - 348y = 1368$

c) $1242x + 1476y = 90$

d) $(4n+1)x + 2ny = n$

e) $(2n+1)x + 4ny = n$

Bautizo: Se dice que dos enteros a y b son congruentes, módulo m, si m divide a la diferencia $a-b$. $(a \equiv b \pmod{m} \Leftrightarrow m \mid a-b)$.

Propiedades:

a) $a \equiv a \pmod{m}$

b) Si $a \equiv b \pmod{m} \Leftrightarrow b \equiv a \pmod{m}$

c) Si $a \equiv b \pmod{m}$ y $b \equiv c \pmod{m} \Rightarrow a \equiv c \pmod{m}$

d) Si $a \equiv b \pmod{m}$ y $c \equiv d \pmod{m} \Rightarrow a \pm b \equiv c \pm d \pmod{m}$ y $ab \equiv cd \pmod{m}$

e) Si $a \equiv b \pmod{m}$ con $0 \leq a < m$ y $0 \leq b < m$, entonces $a = b$

Llc) Demuestra las propiedades d) y e).

Lld) Si a y m son primos relativos entre sí, entonces la congruencia $ax + b \equiv 0 \pmod{m}$ tiene solución. Además si x_1 y x_2 son soluciones, entonces $x_1 \equiv x_2 \pmod{m}$.

Lle) La congruencia $ax + b \equiv 0 \pmod{m}$ tiene solución si y sólo si el máximo común divisor de a y m divide a b.

Teorema Chino del Residuo: Si $m_1, m_2, \ldots, m_k$ son primos relativos dos a dos, entonces las congruencias $x \equiv a_1 \pmod{m_1}$, $x \equiv a_2 \pmod{m_2}, \ldots, x \equiv a_k \pmod{m_k}$ tiene solución común.

Soluciones del Teorema Chino del Residuo: Sea $t_i = \frac{\prod_{j=1}^{k} m_j}{m_i}$, x_i tal que $1 \le x_i < m_i$ y $t_i x_i \equiv 1 \bmod(m_i)$. El número $t = a_1 x_1 t_1 + \ldots + a_n x_n t_n$ es solución del sistema de congruencias y es única en el intervalo $\left[1, \prod_{i=1}^{k} m_i\right]$.

Llf) Resuelve las (los) siguientes (sistemas de) congruencias:

a) $16x - 9 \equiv 0 \pmod{35}$

b) $200x + 315 \equiv 0 \pmod{441}$

c) $(2n+1)x + 7 \equiv 0 \pmod{4n}$

d) $(3n-2)x + 5n \equiv 0 \pmod{9n-9}$

e) $\begin{cases} x \equiv 0 \pmod{3} \\ x \equiv 0 \pmod{8} \end{cases}$

f) $\begin{cases} x \equiv 1 \pmod{25} \\ x \equiv 7 \pmod{35} \end{cases}$

g) $\begin{cases} x \equiv 3 \pmod{17} \\ x \equiv 4 \pmod{21} \\ x \equiv 5 \pmod{25} \end{cases}$

FO5-14) Encuentra las parejas a, b de enteros positivos tales que $[a, b] = 80$.

FO5-16) Encuentra todas las ternas de enteros $0 < a < b < c$ tales que la suma de sus recíprocos es un entero.

FO5-19) Encuentra n, el menor múltiplo positivo de 1991, tal que el producto de sus divisores sea igual a n^{1991}.

FO5-20) Sea a un entero positivo con la propiedad de que si p es un primo que lo divide entonces también es divisible por p^2. Demuestre que tal número es de la forma $a = q^2r^3$ con q, r enteros.

FO5-21) Para que enteros n sucede que, n divide a $(n-1)!$.

FO5-27) Prueba que ninguno de los enteros 1573, 157573, 15757573, etc. es un número primo.

FO5-28) Encuentra todos los números naturales que se pueden escribir de la forma $3n+35m$ con n y m enteros positivos.

F05-29) Encuentra todos los enteros n con la propiedad de que el conjunto $\{n, n+1, n+2, \ldots, n+10\}$ puede ser partido en dos subconjuntos tales que la suma de los números en uno de ellos, es igual a la suma de los números del otro.

F05-30) Determine los enteros positivos a con la propiedad de que el conjunto $M(a) = \{b; b \in N \text{ y } a+b \mid ab\}$, tiene un único elemento.

F05-31) Prueba que el máximo común divisor de $2^n - (-1)^n$ y $2^{n-1} - (-1)^{n-1}$ es igual a 3 para todo n mayor o igual a 2.

F05-33) Prueba que si $A \subset N$ y A tiene tres elementos entonces existen i, j en A tales que 10 divide a $ij(i+j)(i-j)$.

F05-35) Encuentra todos lo números naturales a, b, c, d tales que el producto de cualesquiera dos de ellos sumado con el producto de los otros dos restantes sea igual 1990.

FO5-14) 27 soluciones.
FO5-16) (2,3,6)
FO5-19) $n = 181 \cdot 11^{10} \cdot 2^{180}$.
FO5-21) n no primo y diferente de 4.
FO5-27) 13 es divisor.
FO5-28) Naturales menores o iguales a 70.

F05-29) $n \leq 25$
F05-30) a debe ser primo.
F05-35) $\begin{cases} a = 1 \quad b = 1989 \\ a = 2 \quad b = 993 \\ a = 5 \quad b = 393 \\ a = 10 \quad b = 189 \end{cases}$

Primos de Fermat
Conjetura de Golbach
Teorema de Lagrange
Postulado de Bertrand