3. ARITMETICA MODULAR

3. 1. *Algoritmo de Euclides*

1.1 Demostrar el Algoritmo de Euclides.

Sean $a\ y\ b$ dos números donde $a > b$ y $b \neq 0$; sea q el cociente que se obtiene de dividir el primero por el segundo y, sea *r* el residuo resultante.

Si $a = bq + r$, para $r = 0$, entonces $a \mid b$ ó $a \mid q$.
Si $a = bq + r$, para $r \neq 0$, entonces $(a-r) \mid b$ ó $(a-r) \mid q$.
Si $a = bq' - r'$ con $r' \neq 0$, entonces $(a+r') \mid b$ ó $(a+r') \mid q'$, siendo q' y r' la cifra de cociente y residuo resultantes en la división por exceso.

Haciendo operaciones, obtenemos $b(cq' - q) = r + r'$. Cuando la diferencia entre $q'\ y\ q$ es igual a la unidad $b = r + r'$, si es distinta, $r + r' = b(q + k) - bq = bk$ donde, en función de la suma de los residuos, se pueden determinar los valores de *b* ó *k*, siendo éste el incremento de *q*.

1.2 En una bolsa hay 41 monedas que queremos repartir entre 5 cajas, pero,

a. **Si colocamos 6 monedas en cada caja, nos sobran 7 monedas.**
b. **Si colocamos 7 sobran 11.**
c. **Si colocamos 8 sobran 6.**
d. **Si colocamos 9 faltan 4.**
e. **Si colocamos 10 faltan 9.**

¿Qué consecuencias nos aportan estas distribuciones?

Las consecuencias son las siguientes:

$41 = 5 \cdot 6 + 11 = 5 \cdot 7 + 6$. El incremento en q es 1 luego, $b = r - r' = 11 - 6 = 5$.
$41 = 5 \cdot 6 + 11 = 5 \cdot 8 + 1$. El incremento en q es 2 luego, $b = r - r' = \frac{11-1}{2} = 5$.
$41 = 5 \cdot 6 + 11 = 5 \cdot 9 - 4$. El incremento en q es 3 luego, $b = r + r' = \frac{9+6}{3} = 5$.
$41 = 5 \cdot 6 + 11 = 5 \cdot 10 - 9$. El incremento en q es 4 luego, $b = r + r' = \frac{11+9}{4} = 5$.

Como podemos observar, en las dos últimas igualdades, *b* será igual a la suma de los residuos si éstos tienen signo contrario, o a su diferencia, si son de signos iguales.

1.3 Algunos supuestos de aplicación del Algoritmo de Euclides.

3.1. Si $A = Bq + 7$ y también $A = B(q+1) - 3$, para $A \leqq 100$, determinar los valores de *B* y *q*.

Como $A = Bq + 7 = B(q+1) - 3$ donde $Bq + 7 = B(q+1) - 3$, haciendo operaciones resulta para $B = 10$.

Si $10q + 7 \leqq 100$, $10q \leqq 93$ tenemos para $q \leqq 9$ entonces
$A = 10 \cdot 9 + 7 = 97$ ó $A = 10(9+1) - 3 = 10 \cdot 10 - 3 = 97$

3.2. Si $A=Bq+23$ y también $A=B(q+1)+16$, para $A\leqq 150$, determinar los valores de B y q.

Como $A=Bq+23=B(q+1)+16$ donde $Bq+23=B(q+1)+16$, haciendo operaciones resulta para $B=7$.

Si $7q+23\leqq 150$, $7q\leqq 127$ tenemos para $q\leqq 18$ entonces
$A=7\cdot 18+23=149$ ó $A=7(18+1)+16=7\cdot 19+16=97$

3.3. Si $A=Bq+37$ y $A=B(q+10)-13$, *para* $A\leqq 200$.
Como $A=Bq+37=B(q+10)-13$ donde $Bq+37=B(q+10)-13$, haciendo operaciones, $Bq+10B-13=Bq+37$ resulta para $B=5$.
Si $5q+37\leq 200$, $5q\leq 163$ resulta para $q\leq 32$ entonces
$A=5\cdot 32+37=197$ ó $A=5(32+10)-13=197$.

3.4. Si $A=Bq+47$ y $A=B(q+3)+26$, *para* $A\leqq 61$.
Sea $A=Bq+47=B(q+3)+26$ donde $Bq+47=B(q+3)+26$, haciendo operaciones, $Bq+3B+26=Bq+47$ que resulta para $B=7$.

Si $7q+47\leq 61$, $7q\leq 14$ resulta para $q=2$, entonces
$A=7\cdot 2+47=61$ ó $A=7(2+3)+26=61$.

3. 2. *Congruencias lineales*

2.1 Concepto de congruencia: Propiedades.

Si *a, b* y *m* son números enteros tales que $a-b$ es un múltiplo de *m,* que es positivo, se dice que *a* y *b* son congruentes respecto del módulo m, si la diferencia dividida por él producen el mismo resto.
La relación de congruencia se expresa como $a\equiv b(mód.m)$, relación que fue ideada por Gauss.
Cuando *a* y *b* no sean congruentes respecto del módulo m, escribiremos $a\not\equiv b(mód.m)$.
De la propia definición se deduce que $a-b\equiv 0(mód.m)$. La congruencia puede expresarse como $a=mt+r$ con $0\leq r<m$ donde *t* es un número entero. A esta expresión se le llama *división euclidea en el conjunto* $\mathbb{N}$ *de los números naturales*.
A partir de la definición dada anteriormente, indicamos a continuación las propiedades de las congruencias:

I) Para todo $a\equiv a(mód.m)$, es decir, todo número es congruente consigo mismo, respecto a cualquier módulo: *propiedad reflexiva.*
II) Si $a\equiv b(mód.m)$ entonces $b\equiv a(mód.m)$: *propiedad recíproca*.
III) Si $a\equiv b(mód.m)$ y $b\equiv c(mód.m)$, entonces $a\equiv c(mód.m)$: *propiedad transitiva*.
IV) Si un número *a* es primo con m, todo $b\equiv a(mód.m)$ será también primo con *m*.
V) Si $a\equiv b(mód.m)$ y $c\equiv d(mód.m)$, también $a+c\equiv b+d(mód.m)$.
VI) Si $a\equiv b(mód.m)$ y *c* es distinto a *cero*, entonces $ac\equiv bc(mód.m)$.
VII) Si $a\equiv b(mód.m)$ y *d* es un divisor cualquiera de $a\equiv b(mód.d)$.
VIII) Si $ac\equiv bc(mód.m)$ y el $mcd(c,m)=d$ entonces, $a\equiv b(mód.m/d)$.
IX) Si *k* es un número natural y $a\equiv b(mód.m)$ también $a^k\equiv b^k(mód.m.)$.

X) Si *b* es 1 o b^2 entonces $(m-b)^2 \equiv b^2(mód.m)$.

XI) Si *p* es un número primo entonces $(m+n)^2 \equiv m^p + n^p (mód.p)$.

XII) Si *p* es un número primo, $(m_1 + m_2 + ... + m_n)^2 \equiv {m_1}^p + {m_2}^p + ... + {m_n}^p (mód.p)$.

2.2 Calcular el resto de dividir 213 por 7.

Si tenemos en cuenta el $Algoritmo\ de\ Euclides$, planteamos $213 = 7q + r$ para conocer el cociente *q* y el resto *r*. Si utilizamos congruencias, $213 \equiv r(mód.7)$ para conocer *r*, que es la solución de la congruencia.
Por el $Algoritmo\ de\ Euclides$ la solución es $213 = 7 \cdot 30 + 3$. Aplicando congruencias, $213 \equiv 3(mód.7)$ que representamos como $213 - 3 \equiv 0(mód.7)$ y como $213 - 3 = 210 = 7 \cdot 30$ la solución modular resulta $a = 3 + 7t$.
La solución de este supuesto nos demuestra la estrecha relación que existe entre el $Algoritmo\ de\ Euclides$ y las congruencias.

2.3 Dividir el número 101 en dos partes tales que, una sea múltiplo de 11 y la otra sea múltiplo de 17.

Sean $a\ y\ b$ los números a buscar entonces, se trata de resolver $11a \equiv 101(mód.17)$.
Observamos que $11 < 17 < 101$ por tanto, necesitamos una herramienta que nos permita la solución de este supuesto.
Dado un número *a*, recibe el nombre de *inverso de a módulo m*, otro número a' tal que $aa' \equiv 1(mód.m)$. La condición necesaria y suficiente para que un entero *a* posea un *inverso módulo m*, con $m > 1$, es que el $mcd(a,m) = 1$. Además, ese $inverso$ es ú$nico\ módulo\ m$.
Para determinar el inverso de un número aplicaremos la $Identidad\ de\ Bézout$.
Si tenemos en cuenta que el $mcd(11{,}17) = 1 = 11(-3) + 17(2)$ resulta que los coeficientes 3 y 2 son los inversos de 11 respecto al módulo 17 y de 17 respecto al módulo 11 y también conocidos como $coeficientes\ de\ Bézout$. Aplicando la propiedad recíproca, tenemos.
Para $17b \equiv 101(mód.11)$ donde $2(17a \equiv 101)(mód.17) = 34b \equiv 202(mód.11)$.
Ahora, sacamos restos de 34 y 202 respecto al módulo $11b \equiv 4(mód.11)$ que es equivalente a $b = 4 + 11t$, donde t es un entero cualquiera.
En cuanto al valor de a, por sustitución $101 - (17 \cdot 4) = 101 - 68 = 33$ que resulta para $a = 3 - 17t$ luego, $11(3 - 17t) + 17(4 + 11t) = 101$ es la solución.

2.4 Calcular números congruentes con 13 módulo 7.

Como $x \equiv 13(mód.7)$ es equivalente a $x \equiv 6(mód.7)$, resulta para $x = 13 + 7t$ o bien $x = 6 + 7t$. Dando valores a t, con 13 y 6

t=	**0**	**1**	**2**	**3**	**4**	**…**	**-1**	**-2**	**-3**	**-4**
x=	13	20	27	34	41	…	6	-1	-8	-15

t=	**0**	**1**	**2**	**3**	**4**	**….**	**-1**	**-2**	**-3**	**-4**
x=	6	13	20	27	34	….	-1	-8	-15	-22

obtenemos un conjunto de clases residuales

$$\{\dots, -1.-8, -15, +6, +13, +20, +27, +34, +41, \dots\}$$
$$\{\dots, -1, -8, -15, -22, +6, +13, -20, +27, +34, \dots\}$$

todas de congruencias finitas.

2.5 Comprobar que los enteros menores de 11, excepto el 1 y el 10, pueden agruparse de dos en dos de manera que $x \equiv 1(\mathrm{m\acute{o}d}.\,11)$.

Como *11* es un número primo, todos los elementos no nulos de $\mathbb{Z}_{11,}$ donde $\mathbb{Z}_m$ es un anillo de clases residuales respecto al módulo m, son elementos inversibles.
Los inversos de cada uno quedan expresados en la siguiente lista:

$1 \cdot 1 \equiv 1(mód.\,11)$: 1 es inverso de sí mismo en $\mathbb{Z}_{11}$.
$2 \cdot 6 \equiv 1(mód.\,11)$: 6 es inverso de 2 y 2 es inverso de 3 en $\mathbb{Z}_{11}$.
$3 \cdot 4 \equiv 1(mód.\,11)$: 3 es inverso de 4 y 4 es inverso de 3 en $\mathbb{Z}_{11}$.
$5 \cdot 9 \equiv 1(mód.\,11)$: 5 y 9 son inversos uno del otro en $\mathbb{Z}_{11}$.
$7 \cdot 8 \equiv 1(mód.\,11)$: 7 y 8 son inversos uno del otro en $\mathbb{Z}_{11}$.
$10 \cdot 10 \equiv 1(mód.\,11)$: 10 es inverso de sí mismo en $\mathbb{Z}_{11}$.

2.6 Encontrar un número tal que si se divide por 3, el resto es 2; si se divide por 5, el resto es 3 y, si se divide por 7, el resto es 2

Ya en el siglo III, el matemático chino Sun-Tzi quiso saber este número. En atención a él y otros como Lin Hiu (siglo III), Yang Hui (siglo XI), Chon Huo (siglo XIII), matemáticos chinos que aportaron soluciones a los sistemas de congruencias lineales, hay un teorema llamado $Teorema\ Chino\ del\ Resto$.
Este teorema afirma que, si $m_1, m_2, \dots, m_n$ son enteros positivos, primos relativos dos a dos, el sistema $x \equiv a_1(mód.\,m_1),\ \ x \equiv a_2(mód.\,m_2),\ \ x \equiv a_n(mód.\,m_n)$ tiene solución única $m = m_1 \cdot m_2 \cdot m_n$ esto es, hay una solución $x, 0 \leq x < m$, y todas las demás soluciones son congruentes módulo m con esta solución.
Aplicado a nuestro supuesto, tenemos

Sea $m = 3 \cdot 5 \cdot 7 = 105$. $M_1 = \frac{m}{3} = 35$, $M_2 = \frac{m}{5} = 21$ y $M_3 = \frac{m}{7} = 15$.

Se puede observar que 2 es el inverso de 35 módulo 3, 1 es inverso de 21 módulo 5 y 1 es inverso de 15 módulo 7 por tanto

$x \equiv a_1 M_1 y_1 + a_2 M_2 y_2 + a_3 M_3 y_3$
$x \equiv 2 \cdot 35 \cdot 2 + 2 \cdot 21 \cdot 1 + 2 \cdot 15 \cdot 1 = 233 \equiv 23(mód.\,105)$

Donde el 23 es el número entero más pequeño que al ser dividido por 3, 5 y 7 se obtienen restos respectivos de 2, 3 y 2.

2.7 Resolver la congruencia $17x \equiv 5(\mathrm{m\acute{o}d}.\,13)$.

El coeficiente de $17x$ es mayor que el módulo 13, el resto con éste es $17 = 13 \cdot 1 + 4$ entonces, $4x \equiv 5(mód.\,13)$ es equivalente a $17x \equiv 5(mód.\,13)$.
Si multiplicamos $4x \equiv 5(mód.\,13)$ por 10, $10 \cdot 4x \equiv 10 \cdot 5(mód.\,13)$ y sacamos restos respecto al módulo 13, $x \equiv 11(mód.\,13)$ es la solución de la ecuación, que podemos escribir como $x = 11 + 13t$, donde *t* es un entero cualquiera.
Observar que $17 \cdot 11 = 187 \equiv 5(mód.\,13)$ o $187 - 5 \equiv 0(mód.\,13)$ corresponden a la misma solución de la congruencia.

2.8 Resolver la congruencia $\mathbf{17!} \equiv \boldsymbol{r}(\boldsymbol{m}\acute{\mathbf{o}}\boldsymbol{d}.\mathbf{19})$.

El teorema de $John\ Wilson\ (1741-1793)$ dice.
Para que *n* divida a $((n-1)!+1)$, es necesario y suficiente que *n* sea primo. Para $n>0$ entero primo, tenemos pues que $(p-1)!\equiv -1(mód.p)$.
Si multiplicamos la ecuación $17!\equiv r(mód.19)$ por 18 obtenemos $18!\equiv 18r(mód.19)$ y como $(19-1)!\equiv -1(mód.19)$ equivale a $18r\equiv -1(mód.19)$ esto es $18r\equiv 18(mód.19)$ luego, $r\equiv 1(mód.19)$ y por tanto, $17!\equiv 1(mód.19)$.
La solución resulta r = 1.

2.9 Encontrar solución para $x\equiv a(mód.p)$ y $ax\equiv b(mód.p)$. .

Para $x\equiv a(mód.p)$. Si *p* es primo y *a* es un entero tal que el $mcd(a,p)=1$ entonces, a^{p-2} es inverso de *a* tal que $a^{p-2}\cdot x\equiv b(mód.p)$. Por ejemplo, para $3x\equiv 10(mód.7)$ la solución sería $3^5\cdot 3x=243\cdot 3=729x\equiv 2430(mód.7)$ que equivale a $x\equiv 1(mód.7)$.
Para $ax\equiv b(mód.p)$, si *a* y *b* son enteros, *p* primo y $mcd(a,p)=1$ entonces, la solución vendría determinada por $x\equiv a^{p-2}\cdot b(mód.p)$ qué aplicada a nuestro ejemplo, $x\equiv 3^5\cdot 10\equiv 2430(mód.7)$ y por tanto $x\equiv 1(mód.7)$.

2.10 Demostrar que $\mathbf{10!} \equiv \mathbf{-1}(\boldsymbol{m}\acute{\mathbf{o}}\boldsymbol{d}.\mathbf{11})$.

Tenemos que $10!=10\cdot 9\cdot 8\cdot 7\cdot 6\cdot 5\cdot 4\cdot 3\cdot 2\cdot 1\equiv 10\cdot 8\cdot 7\cdot 6\cdot 4\cdot 3\cdot 2\cdot 1(mód.11)$ ya que $9\cdot 5=45\equiv 1(mód.11)$. Agrupando los factores por pares, 2 y 6, 3 y 4, 7 y 8, tendremos $10!\equiv 10(mód.11)$ y como $10\equiv -1(mód.11)$ entonces, $10!\equiv -1(mód.11)$.

2.11 Resolver el siguiente sistema, $x\equiv b_1(mód.4)$, $x\equiv b_2(mód.5)$ y $x\equiv b_3(mód.7)$ y obtener valores con 1,3,2 y 3,2,6 de $b_1, b_2\ y\ b_3$.

Aquí $4\cdot 5\cdot 7=140$ es equivalente a $35\cdot 4=28\cdot 5=20\cdot 7$ y, además $35\cdot 3\equiv 1(mód.4)$, $28\cdot 2\equiv 1(mód.5)$ y $20\cdot 6\equiv 1(mód.7)$ siendo $x_o=35\cdot 3b_1+28\cdot 2b_2+20\cdot 6b_3$ por consiguiente, el sistema puede expresarse como $x\equiv 105b_1+56b_2+120b_3(mód.140)$.
Para valores de 1, 3, 2 tenemos $x\equiv 105\cdot 1+56\cdot 3+120\cdot 2\equiv 93(mód.140)$ y para valores de 3, 2, 6, $x\equiv 105\cdot 3+56\cdot 2+120\cdot 6\equiv 27(mód.140)$ donde, para los distintos valores, la solución del sistema es de $x=93+140t$ y $x=27+140t$.

2.12 Calcular los valores $b_1, b_2\ y\ b_3$ de la ecuación $\boldsymbol{x}\equiv \mathbf{1000}(\boldsymbol{mód}.\mathbf{1547})$.

Como $1547=7\cdot 13\cdot 17,$ la ecuación propuesta tendrá solución si, y sólo si, la tienen sus factores $x\equiv 1000(mód.7),$ $x\equiv 1000(mód.13)$ y $x\equiv 1000(mód.17)$ que son equivalentes a $x=1000+7t=6+7t,$ $x=1000+13t=12+13t$ y $x=1000+17t=14+17t.$ Aplicando el *Teorema Chino de Restos*, como $1547=7\cdot 221=13\cdot 119=17\cdot 19,$ resulta

$$\begin{cases} 221a_1 \equiv 1(mód.7) \\ 119a_2 \equiv 1(mód.13) \\ 91a_3 \equiv 1(mód.17) \end{cases} \Rightarrow \begin{cases} 4a_1 \equiv 1(mód.7) \\ 2a_1 \equiv 1(mód.13) \\ 6a_1 \equiv 1(mód.17) \end{cases} \Rightarrow \begin{cases} 221 \cdot 2 \equiv 1(mód.7) \\ 119 \cdot 7 \equiv 1(mód.13) \\ 91 \cdot 3 \equiv 1(mód.17) \end{cases}$$

y por tanto, sustituyendo coeficientes, $x \equiv 442b_1 + 833b_2 + 273b_3(mód.1547)$ que, dando valores a *b* y, realizando productos

$$x \equiv 442 \cdot 6 + 833 \cdot 12 + 273 \cdot 14 \equiv 16470 \equiv 1000(mód.1547).$$

3 3. *Congruencias exponenciales*

3.1 Calcular el resto de dividir 2^{13} por 7.

El $Pequeño\ Teorema\ de\ Fermat$ dice que, si *p* es un entero primo y *a* otro entero tal que el $mcd(a,p) = 1$ entonces, $a^{p-1} \equiv 1(mód.p)$. Esta herramienta nos permite dar solución al supuesto planteado sin importar el grado de su raíz ya que *a* recorre todo el conjunto de restos respecto al módulo utilizado.
Como $a^{7-1} = a^6 \equiv 1(mód.7)$ donde puede ser cualquiera de los números que conformar el conjunto de restos {1,2,3,4,5,6} respecto al módulo 7, o sea, $1^6 = 2^6 = 3^6 = 4^6 = 5^6 = 6^6 \equiv 1(mód.7)$. Tenemos que $a^{13} = a^{2\cdot 6+1} = a^{12} \cdot a^1 = a \equiv 1(mód.7)$ de donde el resto de dividir $a^{13}\ por\ 7$ puede ser 1, 2, 3, 4, 5 ó 6, dependiendo del valor que demos a *a*.

3.2 Calcular el resto de dividir 3^{101} por 23.

El sistema reducido de restos, respecto al módulo p, consta de $\frac{p-1}{2}$ restos cuadráticos, los cuales son congruentes con los números $1^2, 2^2, 3^2, \ldots, \left(\frac{p-1}{2}\right)^2$ y de $\frac{p-1}{2}$ no restos cuadráticos. Si a es resto cuadrático respecto al módulo p, se tiene $a^{\frac{p-1}{2}} \equiv 1(mód.p)$; si a no es resto cuadrático respecto al módulo p, entonces $a^{\frac{p-1}{2}} \equiv -1(mód.p)$. Esto se conoce como $Criterio\ de\ Euler$. Según el teorema de Fermat, $x^{p-1} \equiv 1(mód.p)$ luego

$$(a^{(p-1)/2} + 1)(a^{(p-1)/2} - 1) \equiv 0(mód.p).$$

Como

$$3^{\frac{23-1}{2}} = 3^{11} \equiv 1(mód.23) \text{ y } 101 = 11 \cdot 9 + 2 = 99 + 2$$

la solución pasa por resolver

$$3^2 \equiv r(mód.23).$$

Por la propiedad reflexiva sabemos que todo número es congruente de sí mismo ya que si $a \equiv a(mód.m)$ y $a - a \equiv 0(mód.m)$ entonces, $m|0$. Aplicado al supuesto planteado, fácil es deducir que $r = 9$ y, por tanto $3^{101} \equiv 9(mód.23)$.
De haber utilizado la $función\ de\ Fermat$, donde $a^{p-1} \equiv 1(mód.p)$, esto es $3^{22} \equiv 1(mód.23)$ con $101 = 22 \cdot 4 + 13 = 88 + 13$, la solución vendría dada por la resolución de $3^{13} \equiv r(mód.23)$. Como $3^{13} = 3^3 \cdot 3^3 \cdot 3^3 \cdot 3^3 \cdot 3^1 \equiv r(mód.23)$, o sea

$4\cdot 4\cdot 4\cdot 4\cdot 3 = 768 - r \equiv 0(mód.23)$ y si $768 = 23\cdot 33 + 9$ podemos comprobar que el resto vuelve a ser 9.

3.3 Calcular el resto de dividir 3^{25} por 77.

El módulo es $77 = 7\cdot 11$. Para $3^6 \equiv 1(mód.7)$ y para $3^{10} \equiv 1(mód.11)$. Resolvemos para el módulo 7, $3^{25} = 3^{24}\cdot 3^1 = 3 \equiv 3(mód.7)$ equivalente a $x = 3 + 7t$. Para el módulo 11, $3^{25} = 3^{20}\cdot 3^5 = 1 \equiv 1(mód.11)$ equivalente a $x = 1 + 11t$. Como $3 + 7t_1 \equiv 1(mód.11)$ dónde $7t_1 \equiv 9(mód.11)$ y $t_1 \equiv 6(mód.11)$ equivale a $t_1 = 6 + 11t$, aplicamos los resultados obtenidos para despejar $x = 3 + 7(6 + 11t) = 45 + 77t$ luego, la solución del supuesto es $3^{25} \equiv 45(mód.77)$, siendo 45 el resto buscado.
Notar el uso del *Teorema Chino del Resto*.

3.4 Calcular el resto de dividir 2^{37} por 35.

En la ecuación $2^{37} \equiv r(mód.35)$ el módulo es $35 = 5\cdot 7$ por tanto, la aplicación del *teorema de Fermat* no tendría validez para 35 sino para 5 y 7 entonces, $2^4 \equiv 1(mód.5)$ y $2^6 \equiv 1(mód.7)$. Para $2^{37} = 2^{36}\cdot 2^1 = 2 \equiv 2(mód.5)$ que equivale a $x = 2 + 5t$ y para $2^{37} = 2^{36}\cdot 2^1 = 2 \equiv 2(mód.7)$ que equivale a $x = 2 + 7t$. Como $2 + 5t_1 \equiv 2(mód.7)$ que equivale a $t_1 = 0 + 5t$, sustituimos $x = 2 + 5(0 + 7t) = 2 + 35t$ con lo que la solución al problema es $2^{37} \equiv 2(mód.35)$ o sea, el resto es 2.

3.5 Calcular el resto de dividir 125^{4577} por 13.

Tenemos que $125^{4577} \equiv 1(mód.13)$ y $125^{12} \equiv 1(mód.13)$ siendo $4577 = 12\cdot 381 + 5$. Para $125^{4577} = 125^{4572}\cdot 125^5 = 125^5 = (5^3)^5 = 5^{15}$. Aplicando Fermat, $5^{12} \equiv 1(mód.13)$ y, por tanto $5^{15} = 5^{12}\cdot 5^3 \equiv 8(mód.13)$ luego, $125^{4577} \equiv 8(mód.13)$ siendo 8 el resto.

3.6 Probar si $p \pm 1$ es divisible por 10.

Si p es un número primo distinto de 2 y 5 $p^2 \pm 1$, es divisible por 10 resolviendo la congruencia $p^2 \pm 1 \equiv 0(mód.10)$. Para $p = 7,11,13,19$ resulta $7^2 + 1 = 50 \equiv 0(mód.10)$,

$11^2 - 1 = 120 \equiv 0(mód.10)$, $13^2 + 1 = 170 \equiv 0(mód.10)$ y $19^2 - 1 = 360 \equiv 0(mód.10)$.

3.7 Probar que si x, n, a y m son números enteros positivos donde $x \geq 1$ y $m > 1$, si $x \equiv a(mód.m)$ también $x^n \equiv a^n(mód.m)$.

Sea $x \equiv 2(mód.5)$. Como $x = 2 + 5t$, para $t = 1$ sería $x = 2 + 5 = 7$, esto es $x^2 \equiv 2^2(mód.5)$. Y como $7^2 \equiv 2^2(mód.5)$ es equivalente a $49 - 4 = 45 \equiv 0(mód.5)$ que es la solución de ambas congruencias, queda probada la relación entre ambas.
Sea $x^7 \equiv 5^7(mód.11)$. Como $x = 5 + 11t$, para $t = 1$ sería $x = 5 + 11 = 16$, $16^7 \equiv 5^7(mód.11)$ es equivalente a $16^7 - 5^7 = 16 - 5 = 11 \equiv 0(mód.11)$ que es la solución de ambas congruencias.

3.8 Probar que si para cualquier primo *p* se verifica que $a^p \equiv b^p (\mathrm{m\acute{o}d}.\, p)$ entonces, también se verifica para $a^p \equiv b^p (\mathrm{m\acute{o}d}.\, p^2)$.

Sea $x \equiv 2(mód.7)$. Como $x = 2 + 7t$ y para $t = 1$ sería $x = 2 + 7 = 9$, si $x^7 \equiv 2^7(mód.7^2)$ como $9^7 \equiv 2^7(mód.7^2)$ es equivalente a $9^7 - 2^7 = 9 - 2 = 7 \equiv 0(mód.7^2)$ que es la solución de ambas congruencias, queda probada la relación entre ambas.

3.9 Si p es primo y a, b son números enteros entonces, probar que se cumple que $(a + b)^p \equiv a^p + b^p (\mathrm{m\acute{o}d}.\, p)$.

Sea $(4 + 5)^7 \equiv 4^7 + 5^7(mód.7)$. Si $9^7 \equiv 4^7 + 5^7(mód.7)$, haciendo traspasos $9^7 - (4^7 + 5^7) \equiv 0(mód.7)$ que es equivalente a $4782969 - 94509 = 4688460 \equiv 0(mód.7)$. Como $4688460 = 3^2 \cdot 7 \cdot 11 \cdot 83 = 7 \cdot 669780$, queda probado que la solución que satisface a $(4 + 5)^7 \equiv 4^7 + 5^7(mód.7)$ es $(4 + 5)^7 \equiv 2(mód.7)$.
Sea $(2 + 3 + 4 + 5)^5 \equiv 2^5 + 3^5 + 4^5 + 5^5(mód.5)$. Como $14^5 \equiv 4424(mód.5)$, esto es $4^5 \equiv 4(mód.5)$ entonces $1 \equiv 1(mód.5)$ solución que satisface al supuesto.

3.10 Demostrar que el 2821 es un número de Carmichael.

Un número de $Robert\ Carmichael\ (1879 - 1967)$ es un número *n* compuesto tal, que $a^n \equiv a(mód.m)$ si *mcd (a, n) = 1*, o bien $a^{n-1} \equiv 1(mód.n)$ por similitud con el teorema de Fermat, y también. $2^n \equiv 2(mód.n)$. Se conocen como *pseudoprimos*.
Debemos demostrar $a^{2820} \equiv 1(mód.2821)$ para todo *a* primo relativo con 2821. Como $2821 = 7 \cdot 13 \cdot 31$, y si mcd (a, 2821) = 1, entonces *mcd (a, 7) = mcd (a, 13) = mcd (a, 31) = 1*. De acuerdo con Fermat $a^6 \equiv 1(mód.7)$, $a^{12} \equiv 1(mód.13)$ y $a^{30} \equiv 1(mód.31)$, luego, con relación al número propuesto, tenemos

$a^{2820} \equiv (a^6)^{470} \equiv 1(mód.7)$, $a^{2820} \equiv (a^{12})^{235} \equiv 1(mód.13)$ y $a^{2820} \equiv (a^{30})^{94} \equiv 1(mód.31)$.

Finalmente, utilizando el Teorema Chino de Restos, queda demostrado que

$a^{2820} \equiv 1(mód.2821)$ y por tanto, un número de *Carmichael*.

3.11 Demostrar que el 561 es un número de Carmichael.

Si tenemos en cuenta que $561 = 3 \cdot 11 \cdot 17$, aplicando el mismo procedimiento del supuesto anterior, conseguimos saber qué $a^{560} \equiv 1(mód.561)$ y por tanto, es un *pseudoprimo de Carmichael.*
Otros números de Carmichael pueden ser

561,1105,1729,2465,2821,6601,8911,10585,15841,
29341, 41041,46657,52633,62745,63973,75361

3.12 Demostrar que el 2047 pasa el Test de Miller para la base 2.

Sea *n* un entero positivo y sea $n - 1 = 2^s t$, donde *s* es un entero no negativo y *t* es un entero positivo impar. Decimos que *n* pasa el *Test de Miller para la base b,* bien como $b^t \equiv 1(mód.m)$

o como $b^{2/t} \equiv -1(mód.n)$. Se dice que un entero compuesto *n* pasa el *Test de Miller* para menos de *4/n* bases *b*, *1 < b < n*, o también, si *n* es primo y *b* un entero positivo tal que $a \nmid b$. Un entero positivo que pasa el Test de Miller para la base b se llama *pseudoprimo fuerte para la base b*.
Para el número propuesto vemos que $2047 = 23 \cdot 89$, compuesto que podemos descomponer en $2047-1 = 2046 = 2 \cdot 1023$, por lo que $s = 1$ y $t = 1023$. Aplicando congruencias

$$2^{1023} = (2^{11})^{93} = 2048^{93} \equiv 1^{93} \equiv 1(mód.2047)$$

con lo que demostramos que el número 2047 pasa el Test de Miller y, por tanto, es un *p seudoprimo fuerte para la base 2.*

3.13 Demostrar el Teorema de Wolstenholme, para p=13.

El teorema demostrado por Joseph Wolstenholme en 1819 dice que, para cualquier número primo $p > 3$, se cumple las siguientes congruencias

$$(p-1)!(1+1/2+1/3+\ldots+1/p-1) \equiv 0(mód.p^2)$$
$$(p-1)!^2(1+1/2^2+1/3^2+\ldots+1/(p-1)^2) \equiv 0(mód.p)$$

Para el caso de $p = 13$, obtenemos

$$(13-1)! = 479.001.600,\ \sum_{k=1}^{13-1} 1/k = 86021/27720 \text{ y } \sum_{k=1}^{13-1} 1/k^2 = 240505109/153679680$$

de donde

$$479001600 \cdot 86021/21720 \equiv 0(mód.13^2)$$

y

$$(479001600)^2 \cdot (240505109/153679680) \equiv 0(mód.13)$$

Este teorema se amplía diciendo que, para todo primo $p > 5$ se cumple

$$\sum_{k=1}^{p-1} \frac{(p-1)!}{k} \equiv 0(mód.p).$$

3.14 Calcular $1001^{19} \equiv r(mód.301)$.

Para dar solución a este supuesto vamos a utilizar el método de los cuadrados repetidos. Empezamos por escribir el exponente en la forma $19 = 2^4 + 2 + 1$ y operamos de la siguiente forma:

$$1001^2 \equiv 273(mód.301)$$
$$1001^4 = 273^2 \equiv 182(mód.301)$$
$$1001^8 = 182^2 \equiv 14(mód.301)$$
$$1001^{16} = 14^2 \equiv 196(mód.301)$$

$$1001^{18} = 1001^{16} \cdot 1001^{2} = 196 \cdot 273 \equiv 231(mód.301)$$
$$1001^{19} = 1001^{18} \cdot 1001^{1} = 231 \cdot 98 \equiv 63(mód.301)$$

La solución es para $r = 63.$
Se podía haber reducido la base con $1001 \equiv 98(mód.301)$ pero seguiríamos teniendo una operación de $98^{19} \equiv 63(mód.301),$ que es difícil de manejar teniendo en cuenta el módulo.
Este es un método muy utilizado en criptografía.

3. 4. *Funciones aritmeticas*

4.1 Calcular los exponentes de los primos 2, 3 y 5 que figuran en 10!.

Se llama parte entera de un número real al único entero racional denotado *[x]* tal que $[x] \le x < [x]+1$. Si *x* e *y* son reales y *n* un entero estrictamente positivo, se dan los siguientes resultados.

$$a)\ [x+y] = [x]+[y]+e \text{ con } e=0 \text{ ó } e=1$$
$$b)\ [x-y] = [x]-[y]-e \text{ con } e=0 \text{ ó } e=1$$
$$c)\ [x]+\left[x+\frac{1}{n}\right]+...\left[x+\frac{n-1}{n}\right] = [nx]$$
$$d)\ \left[\frac{[nx]}{n}\right] = [x]$$

Aplicado a la solución del supuesto planteado, $e_n = \left[\frac{x}{p}\right]+\left[\frac{x}{p^2}\right]+...+\left[\frac{x}{p^n}\right]$ por tanto

$$e_2 = \left[\frac{10}{2}\right]+\left[\frac{10}{2^2}\right]+\left[\frac{10}{2^3}\right] = 5+2+1 = 8,\ e_3 = \left[\frac{10}{3}\right]+\left[\frac{10}{3^2}\right] = 3+1 = 4,\ e_5 = \left[\frac{10}{5}\right] = 2$$

entonces, $10! = 3628800 = 2^8 \cdot 3^4 \cdot 175 = 2^8 \cdot 3^4 \cdot 5^2 \cdot 7.$
Como queda demostrado, los exponentes de los primos 2, 3 y 5 que figuran en $10!$ son el 8, 4 y 2.

4.2 Calcular los exponentes de los primos mayores a 10 que dividen a 500!.

Para las potencias del primo número 2, aplicando la función de parte entera, tenemos

$$e_2 = \left[\frac{500}{2}\right]+\left[\frac{500}{2^2}\right]+\left[\frac{500}{2^3}\right]+\left[\frac{500}{2^4}\right]+\left[\frac{500}{2^5}\right]+\left[\frac{500}{2^6}\right]+\left[\frac{500}{2^7}\right]+\left[\frac{500}{2^8}\right]$$
$$= 250+125+62+31+15+7+3+1 = 494.$$

Para las potencias del primo número 3

$$e_3 = \left[\frac{500}{3}\right]+\left[\frac{500}{3^2}\right]+\left[\frac{500}{3^3}\right]+\left[\frac{500}{3^4}\right]+\left[\frac{500}{3^5}\right] = 166+55+18+6+2 = 247\ .$$

Para el número 5 tenemos

$$e_5 = \left[\frac{500}{5}\right] + \left[\frac{500}{5^2}\right] + \left[\frac{500}{5^3}\right] = 100 + 20 + 4 = 124$$

y así, siguiendo el mismo procedimiento, obtendremos las del $e_7 = 82,\ e_{11} = 49,\ e_{13} = 40,$ $e_{17} = 30,\ e_{19} = 29,$ etc., hasta conseguir las máximas potencias de 500! mayores a 10, y que son

$$500! = 2^{494} \cdot 3^{247} \cdot 5^{124} \cdot 7^{82} \cdot 11^{49} \cdot 13^{40} \cdot 17^{30} \cdot 19^{27} \cdot 23^{21} \cdot 29^{17} \cdot 31^{16} \cdot 37^{13} \cdot 41^{12} \cdot 47^{10} \cdot s$$

siendo *s* el resto de potencias.

4.3 Definir la Fórmula de Polignac.

La descomposición de una factorial en números primos se conoce como Fórmula de Polignac, que recibe su nombre del matemático francés de Alphonse Polignac (1817-189), aunque dicha fórmula se le atribuye a Adrien Marie Legendre (1752-1833). Esta fórmula se denota como $n! = \prod p^{e_p(n)}$ que es fácil de demostrar, ya que

$$e_p(n) = \frac{n}{p} + \frac{n}{p^2} + \frac{n}{p^3} + \cdots$$

de hecho $\frac{n}{p}$ es un número de múltiplos de p en $n!$. El término $\frac{n}{p^2}$ se añade a la contribución adicional de los múltiplos de p^2, y así sucesivamente.

Por ejemplo, para determinar en cuántos ceros termina 300!, podemos razonar como sigue:
El número de ceros queda determinado por la potencia mayor de 10 que divida a 300! Ya que abundan más los múltiplos de 2 en 300! que los múltiplos de 5, el número de ceros queda determinado por la potencia mayor de 5 que divida a 300! En este caso,

$$\sum_{k=1}^{\infty} \frac{300}{5^k} = \frac{300}{5} + \frac{300}{5^2} + \frac{300}{5^3} + \cdots = 60 + 12 + 2 + 12/5 = 382/5 \approx 74$$

determina que 300! termina con 74 ceros. Fácilmente se puede demostrar el resultado anterior ya que $300! \equiv 0(mód.5^{74})$ y $300! \not\equiv 0(mód.5^{175})$ son distintos.

4.4 Definir las funciones aritméticas.

Hablar de $funciones\ aritméticas$ en general, no es decir demasiado ya que se conoce bajo esta denominación cualquier función cuyo dominio son los naturales de siempre, $f: \mathbb{N} \longrightarrow \mathbb{C}$. La mayor parte de las veces la imagen también estará dentro de $\mathbb{N}$ o de $\mathbb{R}$.
Entre las $funciones\ aritméticas$ tienen especial interés las que dependen de la factorización en primos.
Se dice que una función aritmética f es $multiplicativa$ si $f(nm) = f(n)f(m)$ siempre que n y m sean coprimos.

El teorema fundamental de la aritmética dice que, *cada entero* $n > 1$ *se puede representar como un producto de factores primos de forma única, salvo el orden de sus factores.* Si n se descompone *en* $n = p_1^{e_1} \cdot p_2^{e_2} \cdot \ldots \cdot p_r^{e_r}$ entonces cualquier f multiplicativa verifica

$$f(n) = \prod_{i=1}^{e} f(p_i^{e_i}).$$

4.5 Definir las funciones divisor.

La función $\sigma(n)$ es la suma de todos los números naturales divisores de n. Si p es primo, entonces $\sigma(p^e) = \frac{p^{(e+1)} - 1}{p - 1}$. Esto es así porque los únicos divisores de p^e son las potencias de p^s con $0 \leq s \leq e$. En consecuencia

$$\sigma(p^e) = 1 + p + p^2 + \cdots + p^e = \frac{p^{(e+1)} - 1}{p - 1}$$

Para todo número real o complejo α y todo entero $n \geq 1$ definimos $\sigma_\alpha(n) = \sum_{d|n} d^\alpha$ como la suma de las potencias $\alpha - ésimas$ de los divisores de n. Las funciones así definidas se llaman $funciones\ divisores$.
Para el caso particular de $\sigma_\alpha(p^e)$ si observamos que los divisores de una potencia de un primo p^e son $1, p, p^2, \cdots, p^e$ luego,

$$\sigma_\alpha(p^e) = 1 + p + p^2 + \cdots + p^e = \frac{p^{\alpha(e+1)} - 1}{p^\alpha - 1}$$

Que la función $\sigma_\alpha(n)$ es multiplicativa lo podemos demostrar por medio de un ejemplo:
Si *p* y *q* son números primos entre sí, entonces

$$\sigma_\alpha(pq) = \sigma_\alpha(p) \cdot \sigma_\alpha(q).$$

Si tenemos en cuenta que los únicos divisores de pq son $1, p, q, pq$, desarrollando

$$\sigma_\alpha(pq) = 1 + p + p + pq = (1 + p) + q(1 + p) = (1 + p)(1 + q)$$

de donde

$$\sigma_\alpha(1 + p)(1 + q) = \sigma_\alpha(p) \cdot \sigma_\alpha(q)$$

Si $\sigma_1(3 \cdot 7) = \sigma_1(3) \cdot \sigma_1(7)$ entonces, $\sigma_1(3 \cdot 7) = 1 + 3 + 7 + 21 = 32 = 4 \cdot 8 = \sigma_1(3)\sigma_1(7)$, con lo que queda demostrado que $\sigma_\alpha(n)$ es multiplicativa.

4.6 Calcular la suma de los cuadrados del número 1000.

Como la factorización de $1000 = 2^3 \cdot 5^3$, aplicando la función divisor, se trata de resolver $\sigma_2(2^3 \cdot 5^3) = \sigma_1(2^3) \cdot \sigma_1(5^3)$. La solución la encontramos en

$$\sigma_2(2^3 \cdot 5^3) = \frac{2^{2(3+1)} - 1}{2^2 - 1} \cdot \frac{5^{2(3+1)} - 1}{5^2 - 1} = 85 \cdot 16276 = 1.383.460$$

Si recordamos que el número de divisores es $\tau(n) = (1+e)$, que para nuestro supuesto serían $\tau(2^3 \cdot 5^3) = (1+3)(1+3) = 16$, sumando los cuadrados de todos ellos obtenemos

$$\sigma_2(1000) = 1^2 + 2^2 + 4^2 + 5^2 + 8^2 + 10^2 + 20^2 + 25^2 + 40^2 + 50^2 + \\ + 100^2 + 125^2 + 200^2 + 250^2 + 500^2 + 1000^2 = 1.383.460$$

4.7 Resolver la función $\mu(45)$.

La función de $Augustus\ Ferdinand\ Möbius\ (1790-1868)$ destaca en que $\mu(n) = 0$ si, y sólo si, *n* es divisible por un cuadrado distinto de 1. Las propiedades son que si *n = 1* entonces $\mu(1) = 1$, si $n = p_1 \cdot p_2 \cdot \ldots \cdot p_r$ con p_i primos distintos, entonces $\mu(n) = (-1)^r$ y, si $a^2 \mid n$, para algún $n > 1$ entonces, $\mu(n) = 0$.

El supuesto planteado $\mu(45) = \frac{45}{3^2} = 0$. Si ahora consideramos que $45 = 5 \cdot 9$, entonces $\mu(45) = \mu(5) \cdot \mu(9) = 0$ ya que para $\mu(5) = (-1)^1 = -1$ y para $\mu(9) = 0$ luego $\mu(45) = \mu(5) \cdot \mu(9) = (-1) \cdot 0 = 0$. Con lo que demostramos que la función $\mu(n)$ no sólo es multiplicativa, si no que μ^2 es la función característica de los *libres de cuadrados*, esto es, los no divisibles por ningún cuadrado mayor que 1.

4.8 Resolver por la función $\mu(n)$ los números 1,3,8,15,21,33,98,101,125,301

Aplicando los criterios de la función $\mu(n)$ tenemos,

Número	1	3	8	15	21	33	98	101	125	301	1001
$\mu_{(n)}$	1	-1	0	1	1	1	0	-1	0	1	-1

Hacer notar que, si el número es primo, la función da como resultado -1.

4.9 Resolver la función $\varphi(720)$

La función de $Leonhard\ Euler\ (1707-1783)$ $\phi(n)$ se define para todos los enteros positivos *n* y representa la cantidad de números de la sucesión $\{1, 2, 3, \ldots, n-1\}$ que son coprimos con n. Si la descomposición factorial de *n* es $n = p^a \cdot p^b \cdot \ldots \cdot p^r$, para la función

$$\phi(n) = n\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right) \cdot \ldots \cdot \left(1 - \frac{1}{p_r}\right) \text{ o } \phi(n) = (p_1^{e1} - p_1^{e1} - 1) \cdot \ldots \cdot (p_r^{er} - p_r^{er} - 1)$$

y en particular, $\phi(n^e) = p^e - p^e - 1$ ó $\phi(p) = p - 1$.

Para el supuesto planteado, sabemos que su descomposición factorial es $720 = 2^4 \cdot 3^2 \cdot 5$ entonces,

$$\phi(720) = 720\left(1-\frac{1}{2}\right)\left(1-\frac{1}{3}\right)\left(1-\frac{1}{5}\right) = 720\left(\frac{1}{2}\right)\left(\frac{2}{3}\right)\left(\frac{4}{5}\right)$$

que es igual a

$$\phi(720) = 720\left(\frac{1}{2}\right)\left(\frac{2}{3}\right)\left(\frac{4}{5}\right) = 720\left(\frac{8}{30}\right) = \frac{5760}{30} = 192\,.$$

Este resultado podemos expresarlo como

$$\phi(720) = \phi(16)\cdot\phi(9)\cdot\phi(5) = 16(1/2)\cdot 9(2/3)\cdot 5(4/5) = 8\cdot 6\cdot 4 = 192$$

Demostrándose que la función $\phi(n)$ es multiplicativa.

4.10 Resolver las funciones y $\varphi(221)$ y $\varphi(192)$

La descomposición factorial de $221 = 13\cdot 17$ luego, $\phi(221) = 221(12/13)(16/17)$ que es igual a $\phi(221) = 221(192/221) = 192$ ó $\phi(221) = \phi(13)\cdot\phi(17)$ pero, como los números son primos, individualmente $\phi(221) = (13-1)(17-1) = 12\cdot 16 = 192$.

Para la segunda función, como $192 = 2^6 \cdot 3$ tenemos que $\phi(192) = 192(1/2)(2/3)$ esto es $\phi(192) = 192(2/6) = 64$.

Una de las propiedades de la función $\phi(n)$ es que si *n > 1* entonces, la suma de los enteros positivos menores o iguales a *n* y relativamente primos con *n* es $\tau(p) = \frac{1}{2}n\phi(n)$

A modo de ampliación, utilizamos los números 12 y 16 para demostrar esta propiedad. Para $\phi(12) = 12(1/2)(2/3) = 4$ y para $\phi(16) = 16(1/2) = 8$. La suma de los números primos con *n* será $\tau(12) = 1/2(12\cdot 4) = 24$ y $\tau(16) = 1/2(16\cdot 8) = 64$. Estos números son el {1, 5, 7, 11} y {1, 3, 5, 7, 9, 11, 13, 15} que, como fácilmente se puede comprobar, suman 24 y 64, respectivamente.

4.11 Resolver la ecuación $x^{50} \equiv 1(mód.35)$ aplicando la función $\varphi(35)$

La solución de $x^{50} \equiv 1(mód.35)$ pasa por que la tengan también

$$\begin{cases} x^{50} \equiv 1(mód.5) \\ x^{50} \equiv 1(mód.7) \end{cases} \Rightarrow \begin{cases} x^{50} \equiv 1(mód.5) \\ x^{50} \equiv 1(mód.7) \end{cases}$$

Sabemos que $x^{(5-1)} \equiv 1(mód.5)$ luego, $x^{50} = x^{48+2} = x^{48}\cdot x^2 = x^2 \equiv 1(mód.5)$, que admite como soluciones, $x \equiv 1,4(mód.5)$, o sea, $x_1 = 1+5t$ *y* $x_2 = 4+5t$.

Para $x^{50} \equiv 1(mód.7)$ tenemos $x^{(7-1)} \equiv 1(mód.7)$ *luego*, $x^{50} = x^{48+2} = x^{48}\cdot x^2 = x^2 \equiv 1(mód.7)$, que admite como soluciones, $x \equiv 1,6(mód.7)$, *esto es*, $x_1 = 1+7t$ *y* $x_2 = 6+7t$.

Aplicando el *Teorema Chino de Restos*

$1+5t\equiv 1(mód.7)$. Como $5t\equiv 0(mód.7)$, resulta para $t\equiv 0(mód.7)$ y el valor de *x* vendrá determinado por $x=1+5(0+7t)=1+35t$.

$1+5t\equiv 6(mód.7)$. Como $5t\equiv 5(mód.7)$, resulta para $t\equiv 1(mód.7)$ y el valor de *x* vendrá determinado por $x=1+5(1+7t)=6+35t$.

$4+5t\equiv 1(mód.7)$. Como $5t\equiv 4(mód.7)$, resulta para $t\equiv 5(mód.7)$ y el valor de *x* vendrá determinado por $x=4+5(5+7t)=29+35t$.

$4+5t\equiv 6(mód.7)$. Como $5t\equiv 2(mód.7)$, resulta para $t\equiv 6(mód.7)$ y el valor de *x* vendrá determinado por $x=4+5(6+7t)=34+35t$.

La solución a la ecuación plateada es $x\equiv 1,6,29,34(mód.35)$.
El teorema de Euler dice que, si $m>1$ y el $mcd(a,m)=1$, $a^{\varphi(m)}\equiv 1(mód.m)$.
Como $35=5\cdot 7$ y $\varphi(35)=35(4/5\cdot 6/7)=24$, resulta $a^{\varphi(35)}\equiv 1(mód.35)$ que podemos escribir como $a^{\varphi(24)}\equiv 1(mód.35)$ donde *a* recorre todo el sistema completo de restos respecto al módulo 35.
Se plantea $a^{50}\equiv 1(mód.35)$ pero, $a^{50}=a^{2(24)+2}=a^2\cdot 1^{48}=a^2\equiv 1(mód.35)$. La propiedad *X* de las congruencias dice, que si b es 1 ó b^2 entonces, $(m-b)^2\equiv b^2(mód.m)$.

$(35-1)^2\equiv 1(mód.35)$ donde, $x\equiv 1,34(mód.35)$.

$(35-6)^2\equiv 1(mód.35)$ donde, $x\equiv 6,29(mód.35)$.

Soluciones que son idénticas a las obtenidas utilizando la función de Fermat.

4.12 Demostrar la relación entre $\varphi(n)$ y $\mu(n)$.

Si $n\geqq 1$, tenemos $\varphi(n)=\sum_{d\mid n}\mu(d)\frac{n}{d}$, función de Euler que podemos escribir como

$$\varphi(n)=\sum_{k=1}^{n}\left\lfloor\frac{1}{(n,k)}\right\rfloor$$

donde k recorre todos los enteros $\leqq n$.
Si $n\geqq 1$, tenemos

$$\sum_{d\mid n}\mu(d)=\left\lfloor\frac{1}{n}\right\rfloor=\begin{cases}1 & \text{si n}=1\\ 0 & \text{si n}>1\end{cases},$$

fórmula de la función de Möbius claramente cierta $n=1$. En la suma $\sum_{d\mid n}\mu(d)$ los únicos términos no nulos proceden de $d=1$ y de los divisores de *n* que son producto de primos distintos.
Para un divisor *d* de *n* fijo podemos sumar respecto de todos los *k* tales que $1\leqq k\leqq n$ si, y sólo si, $1\leqq q\leqq n\mid d$, por lo tanto,

$$\varphi(n)=\sum_{d\mid n}\sum_{q=1}^{n\mid d}\mu(d)=\sum_{d\mid n}\mu(d)\sum_{q=1}^{n\mid d}1=\sum_{d\mid n}\mu(d)\frac{n}{d}.$$

4.13 Demostrar la relación entre $\Lambda(n)$ y $\Psi(n)$.

La notación $\Lambda(n)$ se conoce como *función de Mangoldt* en honor a *Hans C.F. von Mangoldt (1854-1925)*, matemático alemán que la adaptó de otra descubierta por *Nikolay Bugáiev (1837-1903)*, matemático ruso que la descubrió. La función Mangoldt se expresa como $\Lambda(n)=\ln(p)$ si $n=p^k$, con p primo y $k\geqq 1$, o $\Lambda(n)=0$, en caso contrario. La función Mangoldt cumple la siguiente identidad donde $\log n=\sum_{d|n}\Lambda(d)$ que es la suma los d que dividen a n.

La notación $\Psi(n)$ se conoce como la segunda *función de Chebyshev* en honor a *Pafnuy L. Chevyshev (1821-1894)*, matemático ruso que la descubrió. Se denota como $\Psi(n)=\sum_{n\leqq x}k\log(p)$ y su relación con la función de Mangoldt $\Lambda(n)$ es que $\Psi(n)=\sum_{n\leqq x}\Lambda(n)$.

Estas funciones se usan frecuentemente en pruebas relacionadas con los números primos.

4.14 Demostrar la solución para $\log 18=\sum_{d|18}\Lambda(d)$.

Como los divisores de 18 son $1,2,3,6,9$ y 18, tenemos que

$$\log 18=\sum_{d|18}\Lambda(d)=\Lambda(1)+\Lambda(2)+\Lambda(3)+\Lambda(6)+\Lambda(9)+\Lambda(18)$$

que es equivalente a

$$\log n=\sum_{d|18}\Lambda(d)=0,\log 2,\log 3,0,\log 3,0=\log(2\cdot 3\cdot 3)=\log 18$$

4.15 Demostrar la relación entre $\Omega(n)$, $\omega(n$ y $\lambda(n)$.

Sea $n=\prod_{i=1}^{k}p_i^{\alpha_i}$ con números primos distintos $p_1,\ldots,p_r$, entonces se define $\Omega(n)=\sum_{i=1}^{r}\alpha_i$ como la función cuenta factores primos, distintos o iguales, en la que se descompone un número como producto. Dado que $\Omega(1)=0$, esta función no es multiplicativa pero, como los factores primos que aparecen en un producto de dos números, *m y n*, son los que aparecen en *m* más los que aparecen en *n*, se tiene $\Omega(m\cdot n)=\Omega(m)+\Omega(n)$ luego, $a^{\Omega(m\cdot n)}=a^{\Omega(m)+\Omega(n)}=a^{\Omega(m)}\cdot a^{\Omega(n)}$, que sí es completamente multiplicativa.

Sea $n=\prod_{i=1}^{\omega(n)}p_i^{\alpha_i}$ y $\Omega(n)=\sum_{i=1}^{\omega(n)}\alpha_i$ como la función que es igual a la cantidad de factores primos diferentes que dividen a *n*. La función $a^{\omega(n)}$ es multiplicativa. Si m y n no tienen factores comunes, los factores primos que los dividen son distintos y entonces $\omega(m\cdot n)=\omega(m)+\omega(n)$ y por tanto $a^{\omega(m\cdot n)}=a^{\omega(m)+\omega(n)}=a^{\omega(m)}a^{\omega(n)}$.

Por ejemplo, $18=2\cdot 3^2$ tiene como solución $\Omega(18)=3$ y $\omega(18)=2$ ya que en el primero son 3 factores, uno repetido y en el segundo son dos factores primos, sin repetición.

Se denota como $\lambda(n)=(-1)^{\Omega(n)}$ la *función Liouville* en honor a $Joseph\ Liouville\ (1809-1882)$, matemático francés que la descubrió. La función $\lambda(n)=(-1)^{\Omega(n)}$ es completamente multiplicativa. Para cada $n\geqq 1$ tenemos

$$\sum_{d|n}\lambda(d)=\begin{cases}1 \text{ si n } \textit{es un cuadrado}\\ 0 \text{ si n } \textit{no es cuadrado}\end{cases},$$

además,

$$\lambda^{-1}(n)=\left|\mu(n)\right| \text{ para todo } n.$$

Para $\sum_{d|18}\lambda(d)=(1,2,3,6,9,18)=\{1,-1,-1,1,1,-1\}=-1$

4.16 Función L de Dirichlet.

Se llama *Serie L de Dirichlet* a la función de la forma $L(s,\chi)=\sum_{n=1}^{\infty}\frac{\chi(n)}{n^s}$, en honor de *Johann Peter Gustav Lejeune Dirichlet (1805-1859)*, matemático alemán, donde χ es un carácter de Dirichlet y s una variable compleja cuyo componente real es >1. Esta función tiene como identidad

$$L(s,\chi)\prod_p\left(1-\frac{\chi(p)}{p^s}\right)^{-1}$$

donde se demuestra que existen un número infinito de números primos en cualquier progresión aritmética de la forma $ax+b$ con $(a,b)=1$.
Un carácter de Dirichlet es una función aritmética completamente multiplicativa $\chi(n)$, tal que existe un entero positivo k con $\chi(n+k)=\chi(n)$ para todo n y $\chi(n)=0$, siempre que el $mcd(n,k)>1$. Para el caso particular de la progresión $4k+1$, donde

$$\chi(n)=\begin{cases}(-1)^{(n-1)/2} & \textit{para n impar}\\ 0 & \textit{para n par}\end{cases}$$

Es decir, $\chi(n)=1$ si $4k+1$, y $\chi(n)=-1$ si $4k+3$.
Es fácil comprobar que $\chi(m\cdot n)=\chi(m)\cdot\chi(n)$.
La función $L(s,\chi)$ se define como

$$L(s,\chi)=\sum_{n=1}^{\infty}\frac{\chi(n)}{n^s}=1-\frac{1}{3^s}+\frac{1}{5^s}-\frac{1}{7^s}+\ldots.$$

La Identidad de Dirichlet toma la forma de

$$\prod_{p_i\cdot p_j}\left(1-\frac{1}{p_i^s}\right)\cdot\ldots\cdot\left(1-\frac{1}{p_j^s}\right)=1-\frac{1}{3^s}+\frac{1}{5^s}-\frac{1}{7^s}+\ldots$$

Donde p_i son números de la forma $4k+1$ y p_j son números de la forma $4k+3$.

3. 5. *Algunas aplicaciones*

5.1 Aplicando la función $h(k)=k(mód.m)$, para $m=111$, asignar posición de memoria $h(k)$ a los números 064212848, 037149212 y 038423721 de un fichero de personal que tiene k como clave.

La función $h(k)=k(mód.m)$ es utilizada por el ordenador central para asignar posiciones de memoria para facilitar accesos o dar información de ficheros.
Para el supuesto planteado, los números asignados serán el 14, 65 y 72.

$$h(064212848)=064212848(mód.111)=14 \quad h(037149212)=037149212(mód.111)=65$$
$$h(038423721)=038423721(mód.111)=72$$

5.2 Aplicando la función $x_{n+1}=(ax_n+c)(mód.m)$, para $m=9, c=4$ y $x_o=3$, calcular una sucesión de números aleatorios.

La función $x_{n+1}=(ax_n+c)(mód.m)$ se utiliza en informática para generar números *pseudoaleatorios*. Los cuatro elementos que intervienen son: el *módulo m*, el *multiplicador a*, el *incremento c* y la *semilla* x_o, con $2\le a<m$, $0\le c<m$ y $2\le x_o<m$ para todo n. El supuesto planteado es muy sencillo. Los ordenadores utilizan los llamados *multiplicadores puros*, con módulo de $2^{31}-1$ y multiplicador de $7^5=16807$. Estos valores generan un cantidad de números aleatorios de $2^{31}-1=2.147.483.648$ antes de que aparezcan repeticiones.
En nuestro caso:

$$x_1=7x_o+4=7\cdot 3+4=25(mód.9)=7,$$
$$x_2=x_1+4=7\cdot 7+4=53(mód.9)=8,$$
$$x_3=7x_2+4=7\cdot 8+4=60(mód.9)=6,$$
$$x_4=7x_3+4=7\cdot 6+4=46(mód.9)=1,$$
$$x_5=7x_4+4=7\cdot 1+4=11(mód.9)=2,$$
$$x_6=7x_5+4=7\cdot 2+4=18(mód.9)=0,$$
$$x_7=7x_6+4=7\cdot 0+4=4(mód.9)=4,$$
$$x_8=7x_7+4=7\cdot 4+4=32(mód.9)=5,$$
$$x_9=7x_8+4=7\cdot 5+4=39(mód.9)=3,$$

Como $x_9=x_o$, y puesto que cada término sólo depende del anterior, esta es la sucesión generada: {3, 7, 8, 6, 1, 2, 0, 4, 5, *3, 7, 8, 6, 1, 2, 0, 4, 5, 3*, ...}.
Nota: Este supuestos aparece en la página 151 de Matemática Discreta del doctor Kenneth H. Rosen.

5.3 Aplicando la función $f(p)\equiv(p+k)mód.27)$, con clave 3, cifre el siguiente mensaje: ME GUSTARÍA ESTUDIAR ALGO.

La función $f(p)\equiv(p+k)mód.27)$, donde p es el número posicional de la letra en el conjunto del alfabeto de un país (caso de España 27) y k la clave de traslación, se utiliza en criptología para codificar o cifrar mensajes. Es necesario que el receptor conozca el número clave. Los primeros usos de la criptología se deben a Julio César, que cifraba sus mensajes secretos

moviendo la posición de cada letra tres posiciones hacia delante, enviando las tres últimas del alfabeto a las tres primeras. Para expresar matemáticamente el proceso de cifrado de César, reemplazamos cada letra *p* por un entero positivo, $p \leq 27$ que, en relación con la clave de traslación k, se obtiene el entero $f(p)$ del conjunto {0, 1, 2, 3,..., 27}, la letra cifrada.
Para cifrar nuestro mensaje, primero confeccionaremos una tabla de valores para el alfabeto español, asignando 0, 10 y 20 a las letras A, K y T.

p	0	1	2	3	4	5	6	7	8	9
0	A	B	C	D	E	F	G	H	I	J
1	K	L	M	N	Ñ	O	P	Q	R	S
2	T	U	V	W	X	Y	Z			

Para cifrar la letra M, $f(m) = (12+3) \equiv 15(mód.27)$. Para cifrar la letra E

$f(e) = (4+3) \equiv 7(mód.27)$ y así sucesivamente para todas las letras del mensaje:

M	**E**	**G**	**U**	**S**	**T**	**A**	**R**	**I**	**A**	**E**	**S**	**T**	**U**	**D**	**I**	**A**	**R**	**A**	**L**	**G**	**O**
12	4	6	21	19	20	0	18	8	0	4	19	20	21	3	8	0	18	0	11	6	15
15	7	9	24	22	23	3	21	11	3	7	22	23	24	6	11	3	21	3	14	9	18
O	**H**	**J**	**X**	**V**	**W**	**D**	**U**	**L**	**D**	**H**	**V**	**W**	**X**	**G**	**L**	**D**	**U**	**D**	**Ñ**	**J**	**R**

El mensaje cifrado será, **OH JXVWDULD HVWXGLDU DÑJR**.

5.4 Con la función $f^{-1}(p) \equiv (p-k)mód.27)$ y utilizando clave 3, desciframos el mensaje anterior OH JXVWDULD HVWXGLDU DÑJR.

La función $f^{-1}(p) \equiv (p-k)(mód.27)$ es inversa a $f(p) \equiv (p+k)mód.27)$ y por tanto, tiene las mismas características, sólo que se opera al revés.
En nuestro caso, el descifrado resulta:

O	**H**	**J**	**X**	**V**	**W**	**D**	**U**	**L**	**D**	**H**	**V**	**W**	**X**	**G**	**L**	**D**	**U**	**D**	**Ñ**	**J**	**R**
15	7	9	24	22	23	3	21	11	3	7	22	23	24	6	11	3	21	3	14	9	18
12	4	6	21	19	20	0	18	8	0	4	19	20	21	3	8	0	18	0	11	6	15
M	**E**	**G**	**U**	**S**	**T**	**A**	**R**	**I**	**A**	**E**	**S**	**T**	**U**	**D**	**I**	**A**	**R**	**A**	**L**	**G**	**O**

5.5 Contestamos al mensaje anterior, clave 7, LZBCKOKH SHBOJHA SHKBRHILA.

Como $f^{-1}(l) \equiv (11-7) \equiv 4(mód.27)$, $f^{-1}(z) \equiv (26-7) \equiv 19(mód.27)$ y LZBCKOKH es equivalente a ESTUDIA..., sigue descifrando y encontrarás en el mensaje un buen consejo.

5.6 Sistema de codificación RSA.

Uno de los sistemas de codificación asimétricos más conocido en todo el mundo es el denominado RSA (iniciales de los creadores Rivest, Shamir y Adelman) y que fue creado en 1977. El RSA consta de dos claves: una pública, que todo el mundo conoce y otra privada. La base del sistema utilizado por sus creadores son los números primos y la dificultad para encontrar la descomposición factorial de un número cualquiera.
Tomando dos números primos, p y q, se genera $n = p \cdot q$. Usando la función de Euler $\varphi(n)$, que nos da el número de números primos con n, obtenemos z.

$$\varphi(n)=\varphi(p\cdot q)=(p-1)(q-1)=z$$

Para generar la clave pública buscamos un número primo e tal que $z>e$ y $mcd(e,z)=1.$ El siguiente paso es encontrar un número d tal que su producto con e se pueda dividir entre z dando como resto $1,$ es decir, que $d\cdot e-1$ sea divisible por $z.$ Como resultado obtenemos dos números e y d que nos permitirán crear nuestro sistema de encriptación. A partir de aquí, el proceso de codificación y decodificación es el siguiente:
El emisor toma un texto normal P y lo convierte en un texto cifrado C mediante la siguiente fórmula:

$$C\equiv P^e(mód.n)$$

El receptor toma el texto C y lo convierte en un texto P mediante la fórmula:

$$P\equiv C^d(mód.n)$$

Ejemplo: para $p=3,\ q=11$ y $n=p\cdot q=3\cdot 11=33\ \ z=\varphi(33)=2\cdot 10=20$ y por tanto un número tal que $mcd(20,e)=1,$ puede ser 7 así, $e=7.$ Buscamos ahora un número tal que $7d-1=20,$ de donde $d=3.$
Ya estamos en disposición de criptografiar el mensaje HOLA:

Letra	P	$C\equiv P^3(mód.33)$	$P\equiv C^7(mód.33)$	Mensaje
H	08	17	08	H
O	15	09	12	O
L	12	12	12	L
A	01	01	01	A

5.7 Calcular la letra de un D.N.I.

Para calcular la letra que corresponde a un D.N.I. se divide el número por 23 y el resto resultante se busca en la siguiente tabla:

Resto	*0*	*1*	*2*	*3*	*4*	*5*	*6*	*7*	*8*	*9*	*10*	*11*	*12*	*13*	*14*	*15*	*16*	*17*	*18*	*19*	*20*	*21*	*22*
Letra	T	R	W	A	G	M	Y	F	P	D	X	B	N	J	Z	S	Q	V	H	L	C	K	E

Si llamamos N al número del D.N.I. y L a la letra, podemos plantear la siguiente ecuación modular.

$$N\equiv L(mód.23)$$

Por ejemplo, para un documento número 37345806, le corresponde la letra $37345806\equiv 16(mód.23).$ Ahora buscamos el número 16 en la tabla y resulta Q por tanto, el documento queda identificado como $37.345.806-Q.$

5.8 Un restaurador necesita adquirir una partida de vinos para su restaurante. Su propósito es hacerse con un lote que incluya vinos de 5, 7, 11 y 17 euros la botella por un coste total de 375 euros. Nos pide consejo para conocer las distintas combinaciones que puede realizar, dando preferencia a cada uno de los vinos seleccionados. ¿Le ayudamos?

Sean x, y, z y s los tipos de vinos de $5,7,11$ y 17 euros la botella con lo que podemos establecer la siguiente ecuación, $5x+7y+11z+17s=375$. Como $mcd(5,7,11,17)=1$ y 1|375, la ecuación tiene solución en la forma $5x+7y=375-11z-17s,$ donde hemos tomado *x, y* como variables principales y *s, z* como variables libres. Operamos sobre la ecuación general

$$x=5(3+7t)\Rightarrow x=3(375-11z-17s)+7t$$
$$y=7(-2-5t)\Rightarrow y=-2(375-11z-17s)-5t$$

Hacemos operaciones

$$x=3(375-11z-17s)+7t=5-33z-51s+7t$$
$$y=-2(375-11z-17s)-5t=50+22z+34s-5t$$

Ajustamos coeficientes

$$x=5-33z-51s+7t=5+2z-2s+7t$$
$$y=50+22z+34s-5t=50-3z-s-5t$$

Y finalmente obtenemos la solución paramétrica al sistema planteado

$$x=5+2z-2s+7t$$
$$y=50-3z-s-5t$$
$$z=\quad z$$
$$s=\quad\quad s$$

Para determinar el peso específico que puede ejercer en los lotes cada uno de los precios que lo componen, procedemos a calcular sus clases, dando valores a las distintas variables que nos han servido como parámetro:

$Parámetros: z,s,t$	*Botellas*				*Importe*			
$x=5+2z-2s+7t$	68	5	38	42	340	25	190	210
$y=50-3z-s-5t$	1	46	2	5	7	322	14	35
$z=\quad z$	1	1	14	1	11	11	154	11
$s=\quad\quad s$	1	1	1	7	17	17	17	119
Botellas/importe	**71**	**53**	**55**	**55**	**375**	**375**	**375**	**375**

5.9 **Resolver la ecuación $x^n\equiv a(mód.m)$ teniendo en cuenta que: $m>x>n$, $m+n+x\leqslant 30$ y $m\cdot n\cdot x\geqslant 100,$ siendo todos ellos primos. Tomar los valores de a^2 y buscar un número que al ser dividido por *x* dé cómo resto los valores de a^2.**

Empecemos por calcular cuáles serán los valores de $m, x\ y\ z$ que tengan las características requeridas en el enunciado:

m	23	19	19	19	19	19	17	17	17	17	13	13	13	13	13
x	5	7	7	5	5	3	11	7	7	7	11	11	11	7	7
n	2	2	3	2	3	2	2	2	3	5	2	3	5	2	5
S	***30***	***28***	***29***	***26***	***27***	***24***	***30***	***26***	***27***	***29***	***26***	***27***	***29***	***22***	***25***
P	***230***	***266***	***399***	***190***	***285***	***114***	***374***	***238***	***357***	***595***	***285***	***429***	***715***	***182***	***455***
a	**2**	**11**	**1**	**6**	**11**	**9**	**2**	**15**	**3**	**11**	**4**	**5**	**7**	**10**	**11**

Hay tres combinaciones más, pero no se ajustan a lo que demanda el enunciado.
Como podemos comprobar, los restos 9 y son cuadrados perfectos que corresponden a

$$3^2 \equiv 9(mód.19) \text{ y } 11^2 \equiv 4(mód.13).$$

Calculamos las x finales

$$(19-3)^2 = 16^2 \equiv 9(mód.19) \text{ y } (13-2)^2 = 11^2 \equiv 4(mód.13)$$

que son equivalentes a

$$x = 9+19t \text{ y } x = 4+13t.$$

Aplicando el *Teorema Chino de Restos* obtenemos $x = 199+247t$ que como se puede comprobar, si lo dividimos por 19 o por 13 da como restos 9 y 4, respectivamente.

BIBLIOGRAFIA

BIRKOHFF, G. y MACLANE, S., Álgebra Moderna, ISBN: 84-316-1226-6
CLAPHAM, Christopher, Oxford Dictionary of Mathematics, ISBN: 84-89784-56-6
KOBLITZ, Neal, A Course in Number Theory and Cryptography, ISBN: 0-387-94293-9
MUÑOZ, José Luís, Riemann una visión nueva de la geometría ISBN: 10-84-96566-27-7
ROSEN, Kenneth H. Matemática Discreta, ISBN: 84-481-4073-7
TATTERSALL, James J. Elementary Number Theory in Nine Chapters, ISBN: 0-521-61524-0
VINOGRADOV, Iván M., Fundamentos de la Teoría de los Números

APOYO INTERNET

http://hojamat.es/sindecimales/congruencias/inicongruencias.htm
http://es.wikipedia.org/wiki/Aritm%C3%A9tica_modular
http://mathworld.wolfram.com/ModularArithmetic.html
http://mathworld.wolfram.com/Congruence.html
http://mathworld.wolfram.com/Residue.html
http://mathworld.wolfram.com/DivisorFunction.html
http://es.wikipedia.org/wiki/Funci%C3%B3n_L_de_Dirichlet
http://wims.unice.fr/wims/wims.cgi?module=tool/arithmetic/bezout.en (Programa matemático)
http://www.wolframalpha.com/examples/ (Programa matemático)
http://www.vitutor.com/index.html