N1

Números enteros. Divisibilidad. Números primos. Congruencias

1. Algoritmo de la división. Divisibilidad en $\mathbb{Z}$
2. Máximo común divisor. Mínimo común múltiplo
3. Números primos. Teorema fundamental de la Aritmética
4. Divisores y múltiplos de un número natural
5. Congruencias
6. El Pequeño Teorema de Fermat y el Teorema de Wilson

1. Algoritmo de la división. Divisibilidad en

1.1. Algoritmo de la división: *Dados* $a,b \in \mathbb{Z}$ *con* $b > 0$, *existen dos únicos números enteros q y r, llamados respectivamente cociente y resto de la división de a por b, tales que*

$$a = bq + r\,, \qquad con \quad 0 \le r < b$$

1.2. Relación de divisibilidad en : Un número entero $a \ne 0$ es *divisor* de otro número entero b, y se escribe $a\,|\,b$, si existe algún número entero c tal que $b = ac$.

1.3. Ejemplo: Demuestre que el cociente $\frac{a(a^2+2)}{3}$ es un número entero, para cada $a \in \mathbb{Z}$.

SOLUCIÓN: Según el Algoritmo de la División, cualquier entero a, después de dividirlo por 3, resulta ser de una de las formas $3k$, $3k+1$ o $3k+2$, donde $k \in \mathbb{Z}$. Así, si $a = 3k$, será

$$\frac{a\cdot(a^2+2)}{3} = \frac{3k\cdot(9k^2+2)}{3} = k(9k^2+2) \in \mathbb{Z}$$

Si $a = 3k+1$, entonces

$$\frac{a\cdot(a^2+2)}{3} = \frac{(3k+1)[(3k+1)^2+2]}{3} = \frac{(3k+1)(9k^2+6k+3)}{3} = (3k+1)(3k^2+2k+1) \in \mathbb{Z}$$

Por último, si $a = 3k+2$,

$$\frac{a\cdot(a^2+2)}{3} = \frac{(3k+2)[(3k+2)^2+2]}{3} = \frac{(3k+2)(9k^2+12k+6)}{3} = (3k+2)(3k^2+4k+2) \in \mathbb{Z}$$

Por tanto, $\frac{a(a^2+2)}{3} \in \mathbb{Z}$ sea cual sea el número entero a.

2. Máximo común divisor y mínimo común múltiplo

2.1. Máximo común divisor: Sean a y b dos números enteros no ambos nulos. El *máximo común divisor* de a y b, que se escribe $\operatorname{mcd}(a,b)$, es el mayor número entero que divide a ambos. Cuando es $\operatorname{mcd}(a,b)=1$, de dice que a y b son *primos relativos*.

En otras palabras, $\operatorname{mcd}(a,b)$ es el único número entero positivo d que cumple las dos condiciones:

i) $d\,|\,a$ y $d\,|\,b$ ii) Si $c\in\mathbb{Z}$ es tal que $c\,|\,a$ y $c\,|\,b$, entonces $c\le d$.

2.2. Propiedades del máximo común divisor: *En todas ellas, a, b y c son números enteros y a y b no simultáneamente nulos, salvo en i), donde sólo es $a\ne 0$.*

1. $\operatorname{mcd}(a,0)=|a|$, $\operatorname{mcd}(a,a)=|a|$, $\operatorname{mcd}(1,a)=1$
2. $\operatorname{mcd}(a,b)=\operatorname{mcd}(a,-b)=\operatorname{mcd}(-a,b)=\operatorname{mcd}(-a,-b)$
3. $\operatorname{mcd}(a+kb,b)=\operatorname{mcd}(a,b)$, *para cualquier* $k\in\mathbb{Z}$.
4. $\operatorname{mcd}(ka,kb)=|k|\operatorname{mcd}(a,b)$, *para cada* $k\in\mathbb{Z}$, $k\ne 0$.
5. $\operatorname{mcd}(a^2,b^2)=[\operatorname{mcd}(a,b)]^2$
6. *Si* $\operatorname{mcd}(a,b)=1$ *y* $\operatorname{mcd}(a,c)=1$, *entonces* $\operatorname{mcd}(a,bc)=1$.

2.3. Ejemplo: Calcúlese $\operatorname{mcd}(2a+1,\ 9a+4)$, donde a es cualquier número entero.

SOLUCIÓN: Aplicando repetidamente la propiedad 3, se tiene que:

$$\operatorname{mcd}(2a+1,9a+4)=\operatorname{mcd}(2a+1,9a+4-4(2a+1))=\operatorname{mcd}(2a+1,a)=\operatorname{mcd}(2a+1-2a,a)=\operatorname{mcd}(1,a)=1$$

2.4. Ejemplo: Demuestre que si los números enteros a y b son primos entre sí, también lo son $a+b$ y ab.

SOLUCIÓN: Por la propiedad 3, $\operatorname{mcd}(a+b,b)=\operatorname{mcd}(a,b)=1$ y $\operatorname{mcd}(a+b,a)=\operatorname{mcd}(b,a)=1$. De ello y de la propiedad 6 se deduce que $\operatorname{mcd}(a+b,ab)=1$, que es tanto como decir que $a+b$ y ab son primos entre sí.

2.5. Identidad de Bezout: *Dados dos números enteros a y b, no ambos nulos, existen otros dos números enteros x e y tales que*

$$\operatorname{mcd}(a,b)=ax+by \ \blacksquare$$

Los enteros x e y, que no son únicos (véase documento N2), pueden determinarse recorriendo hacia atrás el Algoritmo de Euclides para la división de a por b.

2.6. Ejemplo: Calculamos el máximo común divisor de 506 y 352 y obtenemos dos números enteros x e y tales que

$$\operatorname{mcd}(506,352)=506x+352y\,.$$

SOLUCIÓN: Las divisiones sucesivas que componen el Algoritmo de Euclides son:

$$506=1\cdot 352+154\,,\qquad 352=2\cdot 154+44\,,\qquad 154=3\cdot 44+22\,,\qquad 44=2\cdot 22$$

Cualquiera que sea la manera de expresar los cálculos, se obtiene que:

$$\operatorname{mcd}(506,352)=\operatorname{mcd}(352,154)=\operatorname{mcd}(154,44)=\operatorname{mcd}(44,22)=22$$

Obtenemos los coeficientes enteros x e y tales que $22 = 506x + 352y$. Leemos ahora las sucesivas divisiones efectuadas de atrás hacia delante, exceptuando la última. La tercera se puede escribir $22 = 154 - 3 \cdot 44$, y si en ella sustituimos 44 por su valor en la segunda igualdad. Resulta: $22 = 154 - 3 \cdot 44 = 154 - 3 \cdot (352 - 2 \cdot 154) = 7 \cdot 154 - 3 \cdot 352$. Si ahora sustituimos 154 por su valor en la primera, queda:

$$22 = 7 \cdot 154 - 3 \cdot 352 = 7 \cdot (506 - 352) - 3 \cdot 352 = 7 \cdot 506 - 10 \cdot 352$$

2.7. Caracterización de los primos relativos: *Dos números enteros a y b, no ambos nulos, son primos relativos si y sólo si existen dos enteros x e y tales que $1 = ax + by$.*

2.8. Ejemplo: Demuestre que si $n \in \mathbb{N}$ no es cuadrado perfecto, $\sqrt{n}$ es irracional.

SOLUCIÓN: Supongamos que $\sqrt{n}$ fuese racional, esto es, que existiesen $p, q \in \mathbb{N}$ primos relativos tales que $\sqrt{n} = \frac{p}{q}$. En tal caso serían $p = q\sqrt{n}$ y $p\sqrt{n} = qn$ y además, por ser p y q primos relativos, existirían $x, y \in \mathbb{Z}$ tales que $px + qy = 1$, así que

$$\sqrt{n} = 1 \cdot \sqrt{n} = (px + qy) \cdot \sqrt{n} = (p\sqrt{n})\,x + (q\sqrt{n})\,y = qnx + py \in \mathbb{Z}$$

y entonces $n = (qnx + py)^2$ sería un cuadrado perfecto, contra la hipótesis.

2.9. Corolario 1: *Si* $\operatorname{mcd}(a,b) = d$, *entonces* $\operatorname{mcd}\left(\frac{a}{d}, \frac{b}{d}\right) = 1$.

2.10. Corolario 2 (Lema de Euclides): *Si a, b y c son números enteros tales que $a|bc$ y $\operatorname{mcd}(a,b) = 1$, entonces $a|c$.*

2.11. Ejemplo: Halle dos números enteros positivos sabiendo que su máximo común divisor es 120 y que la diferencia de sus cuadrados es 345600.

Este problema es el 98.17 del volumen 4 de Problemas de oposiciones de Editorial Deimos y allí figura resuelto.

SOLUCIÓN: Sean $A, B \in \mathbb{N}$, $A > B$, los números buscados. Como $\operatorname{mcd}(A,B) = 120$, según 2.9 serán $A = 120a$, $B = 120b$ y $\operatorname{mcd}(a,b) = 1$. La diferencia de sus cuadrados es

$$345600 = A^2 - B^2 = 120^2(a^2 - b^2) = 14400(a^2 - b^2) \quad \Rightarrow \quad a^2 - b^2 = 24$$

es decir, $(a+b)(a-b) = 24$. Por tanto, como $a+b$ y $a-b$ son números de la misma paridad y $a-b < a+b$, se da alguna de las dos posibilidades siguientes:

$$\begin{cases} a-b=2 \\ a+b=12 \end{cases}, \qquad \begin{cases} a-b=4 \\ a+b=6 \end{cases}$$

En el primer caso son $a = 7$ y $b = 5$, y una solución son los números $A = 120 \cdot 7 = 840$ y $B = 120 \cdot 5 = 600$. En el segundo caso son $a = 5$ y $b = 1$, obteniéndose como solución los números $A = 120 \cdot 5 = 600$ y $B = 120 \cdot 1 = 120$.

2.12. Mínimo común múltiplo: El *mínimo común múltiplo* de dos números enteros no nulos a y b, escrito $\operatorname{mcm}(a,b)$, es el único número entero positivo m tal que:

i) $a|m$ y $b|m$.

ii) Si c es un número natural tal que $a|c$ y $b|c$, entonces $m \le c$.

Tal y como se hizo con el máximo común divisor, en la anterior definición puede cambiarse la condición $m \le c$ por $m \mid c$, obteniéndose una definición equivalente.

2.13. Teorema: *Para cualesquiera dos números enteros no nulos a y b ocurre que*

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

2.14. Propiedades del mínimo común múltiplo: *Sean a y b dos números enteros no nulos. Se cumple entonces que:*

1. $\text{mcm}(1,a) = \text{mcm}(a,a) = |a|$
2. $\text{mcm}(a,b) = \text{mcm}(a,-b) = \text{mcm}(-a,b) = \text{mcm}(-a,-b)$
3. $\text{mcm}(ka,kb) = |k|\,\text{mcm}(a,b)$, *para cualquier entero no nulo* k.
4. $\text{mcm}(a^2,b^2) = [\text{mcm}(a,b)]^2$
5. $\text{mcm}(a,b) = |ab|$ *si y sólo si* $\text{mcd}(a,b) = 1$.
6. $\text{mcm}(a,b) = \text{mcd}(a,b)$ *si y sólo si* $a = \pm b$.

2.15. Ejemplo: Calcule dos números enteros positivos cuyo máximo común divisor es 8 y cuyo mínimo común múltiplo es 504.

SOLUCIÓN: Si A y B son los enteros positivos que se buscan, siendo $A > B$, serán $A = 8a$ y $B = 8b$, donde los enteros positivos a y b son primos entre sí. Entonces:

$$504 = \text{mcm}(A,B) = \text{mcm}(8a,8b) = 8 \cdot \text{mcm}(a,b) = 8ab \quad \Rightarrow \quad 63 = ab\,.$$

Por tanto, como es $a > b$, sólo pueden ser $a = 63$, $b = 1$, o bien, $a = 9$, $b = 7$. En el primer caso se obtienen $A = 8 \cdot 63 = 504$ y $B = 8 \cdot 1 = 8$, mientras que en el segundo caso son $A = 8 \cdot 9 = 72$ y $B = 8 \cdot 7 = 56$.

3. Números primos. Teorema fundamental de la aritmética

3.1. Definición: Un número entero $p>1$ se dice *primo* si sus únicos divisores positivos son 1 y p. Un número entero mayor que 1 que no es primo se llama *compuesto*.

3.2. Ejemplo (Teorema de Sophie Germain): Demuestre que el número n^4+4 es compuesto, para cada número entero $n\geq 2$.

Este problema figura resuelto en la página 519 del volumen 3 de Problemas de Oposiciones de Editorial Deimos.

SOLUCIÓN: Completamos cuadrados, lo que permitirá expresar n^4+4 como diferencia de cuadrados, es decir, como suma por diferencia:

$$n^4+4=(n^4+4n^2+4)-4n^2=(n^2+2)^2-(2n)^2=(n^2+2n+2)(n^2-2n+2)$$

Si el último factor (el menor de ambos) fuese 1, es decir, si $n^2-2n+2=1$, entonces $n^2-2n+1=0$, o bien, $(n-1)^2=0$, luego $n=1$, pero esto es imposible por hipótesis. Por tanto, n^4+4 es el producto de dos factores positivos mayores que 1, es decir, n^4+4 es compuesto.

3.3. Teorema: *Si p es un número primo y $p\,|\,ab$, entonces $p\,|\,a$ o $p\,|\,b$.*

Esta propiedad fundamental de los números primos no la tienen, en general, los números compuesto. Obsérvese que si un número entero c no es primo, es decir, si c es compuesto y además es divisor del producto ab, puede ocurrir que c no divida a ninguno de los factores a o b. No hay que ir muy lejos para comprobarlo: 6 es divisor de $4\cdot 3=12$ y, en cambio, 6 no divide ni a 4 ni a 3.

El *Teorema fundamental de la Aritmética*, que ahora se enuncia, establece que todo número entero mayor que 1 es divisible por algún número primo y permite expresarlo en su forma canónica.

3.4. Teorema fundamental de la Aritmética: *Cada número entero $n > 1$ puede ser expresado como producto de números primos de forma única, salvo el orden de escritura de los factores.*

Algunos de los números primos que aparecen en la factorización de un entero positivo pueden estar repetidos. Agrupándolos en potencias, se establece el siguiente…

3.5. Corolario 1 (Factorización canónica de un número entero positivo): *Cualquier entero positivo $n > 1$ puede factorizarse de modo único en su "forma canónica"*

$$n = p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r}$$

donde cada k_i es un número entero positivo, cada p_i es un número primo y $p_1 < p_2 < \cdots < p_r$.

3.6. Corolario 2 (Euclides): *El conjunto de los números primos es infinito.*

DEMOSTRACIÓN: Razonamos por reducción al absurdo. Supongamos que sólo hubiese una cantidad finita $p_1, p_2, \ldots, p_n$ de números primos, donde $1 < p_1 < p_2 < \cdots < p_n$. Considérese entonces el entero positivo

$$N = p_1 p_2 \cdots p_n + 1 .$$

Como es $N > 1$, según el Teorema fundamental, N es divisible por algún número primo, pero dado que los únicos números primos son $p_1, p_2, \ldots, p_n$, el entero positivo N es divisible por alguno de los p_j, de modo que será $N = a p_j$, para cierto $a \in \mathbb{Z}^+$ y algún $j = 1, \ldots, n$, es decir, $p_1 p_2 \cdots p_n + 1 = a p_j$, o bien, $a p_j - p_1 p_2 \cdots p_n = 1$, esto es, $p_j \left(a - p_1 \cdots p_{j-1} p_{j+1} \cdots p_n\right) = 1$, pero aquí dice que p_j es divisor positivo de 1, es decir, que $p_j = 1$, pero esto es falso por ser p_j un número primo. En consecuencia, el conjunto de los números primos es infinito.

3.7. Ejemplo: Demuestre que si el producto de dos enteros positivos a y b primos entre sí es la potencia n-ésima de un número entero positivo $(n \geq 2)$, entonces cada uno de los factores a y b es asimismo potencia n-ésima de un entero positivo.

SOLUCIÓN: Supongamos que es $ab = c^n$, donde $c \in \mathbb{N}$. Si fuesen $a = 1$ o $b = 1$, la cuestión es inmediata. Si, en cambio, son $a, b > 1$ y las factorizaciones canónicas de a y b son

$$a = p_1^{\alpha_1} \cdots p_r^{\alpha_r} \qquad \text{y} \qquad b = q_1^{\beta_1} \cdots q_s^{\beta_s},$$

entonces $p_i \neq q_j$ para todos los $i = 1, \ldots, r$ y $j = 1, \ldots, s$, por ser a y b primos entre sí, de manera que

$$ab = p_1^{\alpha_1} \cdots p_r^{\alpha_r} q_1^{\beta_1} \cdots q_s^{\beta_s}$$

es, salvo el orden de escritura de los factores, la factorización canónica del número entero positivo ab. Ahora bien, como ab es potencia n-ésima, cada uno de los exponentes de dicha factorización es múltiplo de n, es decir, $\alpha_i = na_i$ y $\beta_j = nb_j$ para $i = 1, \ldots, r$ y $j = 1, \ldots, s$, luego

$$a = p_1^{\alpha_1} \cdots p_r^{\alpha_r} = p_1^{na_1} \cdots p_r^{na_r} = (p_1^{a_1} \cdots p_r^{a_r})^n \quad \text{y} \quad b = q_1^{\beta_1} \cdots q_s^{\beta_s} = q_1^{nb_1} \cdots q_s^{nb_s} = (q_1^{b_1} \cdots q_s^{b_s})^n$$

son potencias n-ésimas de números enteros positivos ■

Nótese que el cumplimiento de la propiedad anterior requiere que los enteros positivos a y b sean primos relativos. Considérense, por ejemplo, las siguientes factorizaciones de 36, que es un cuadrado perfecto:

$$36 = 4 \cdot 9 = 2 \cdot 18.$$

En la primera de ellas 4 y 9 son primos relativos y por tanto cuadrados perfectos. En la segunda, 2 y 18 no son primos relativos (tienen al dos como divisor común) y ninguno de ambos es cuadrado perfecto.

A partir del Teorema fundamental se identifican ahora los divisores de un entero positivo n en función de los distintos primos p_i que dividen a n, y se dan expresiones abreviadas para determinar su número, su suma y su producto.

4. Divisores y múltiplos de un entero positivo

4.1. Divisores positivos de un entero positivo. Número, suma y producto: *Si* $n = p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r}$ *es la descomposición canónica del entero positivo* $n > 1$ *, entonces:*

i) *Los divisores positivos de n son los números*

$$d = p_1^{a_1} p_2^{a_2} \cdots p_r^{a_r} ,$$

donde $0 \le a_i \le k_i$ *, para cada* $i = 1,2,\ldots,r$ *.*

ii) *El número* $\tau(n)$ *de divisores positivos de n es*

$$\tau(n) = (k_1 + 1)(k_2 + 1)\cdots(k_r + 1)$$

iii) *La suma* $\sigma(n)$ *de los divisores positivos de n es*

$$\sigma(n) = (1 + p_1 + \cdots + p_1^{k_1})\cdots(1 + p_r + \cdots + p_r^{k_r}) = \frac{p_1^{k_1+1} - 1}{p_1 - 1} \cdots \frac{p_r^{k_r+1} - 1}{p_r - 1}$$

iv) El producto de los divisores positivos de n es

$$n^{\tau(n)/2}$$

4.2. Observación: Las fórmulas anteriores para el número de divisores de un entero positivo n, su suma o su producto siguen siendo válidas cuando n se factoriza en la forma:

$$n = p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r}$$

donde los p_i son números primos y algunos exponentes k_i son nulos. Obsérvese para ello que si suponemos que los únicos exponentes no nulos son los j primeros, es decir, si $k_i > 0$ para $i = 1, \ldots, j$ y $k_{j+1} = \cdots = k_r = 0$, entonces $k_{j+1} + 1 = \cdots = k_r + 1 = 1$ y

$$\tau(n) = \tau(p_1^{k_1} p_2^{k_2} \cdots p_j^{k_j}) = (k_1+1)(k_2+1)\cdots(k_j+1) = (k_1+1)(k_2+1)\cdots(k_j+1)(k_{j+1}+1)\cdots(k_r+1) = (k_1+1)(k_2+1)\cdots(k_r+1)$$

Dado que también $1 + p_{j+1} + \cdots + p_{j+1}^{k_{j+1}} = \cdots = 1 + p_r + \cdots + p_r^{k_r} = 1$, se deduce que

$$\sigma(n) = \sigma(p_1^{k_1} p_2^{k_2} \cdots p_j^{k_j}) = (1 + p_1 + \cdots + p_1^{k_1})\cdots(1 + p_j + \cdots + p_j^{k_j}) = (1 + p_1 + \cdots + p_1^{k_1})\cdots(1 + p_r + \cdots + p_r^{k_r})$$

4.3. Ejemplo: Halle un número entero positivo A cuyos únicos factores primos son 2, 5 y 7, sabiendo que $5A$ y $8A$ tienen, respectivamente, 8 divisores positivos y 18 divisores positivos más que A. Calcule también la suma de todos los divisores positivos de A.

SOLUCIÓN: Si $A = 2^a \cdot 5^b \cdot 7^c$, donde $a, b, c \in \mathbb{N}^+$, es la factorización canónica del entero positivo que se busca, las correspondientes de $5A$ y $8A$ son $5A = 2^a \cdot 5^{b+1} \cdot 7^c$ y $8A = 2^{a+3} \cdot 5^b \cdot 7^c$. Según el enunciado:

$$\begin{cases} (a+1)(b+2)(c+1) - (a+1)(b+1)(c+1) = 8 \\ (a+4)(b+1)(c+1) - (a+1)(b+1)(c+1) = 18 \end{cases} \Leftrightarrow \quad \begin{cases} (a+1)(c+1) = 8 \\ (b+1)(c+1) = 6 \end{cases}$$

De la última doble igualdad se deduce que $c+1$ es divisor de 8 y de 6, es decir, que $c+1$ es divisor de $\text{mcd}\,(8,6)=2$. Dado que $c+1\geq 2$, necesariamente es $c+1=2$, luego $c=1$ y por tanto $a=3$ y $b=2$, con lo que el número que se buscaba era

$$A=2^3\cdot 5^2\cdot 7=1400\,.$$

La suma de los divisores de A es

$$\sigma\,(A)=(1+2+2^2+2^3)(1+5+5^2)(1+7)=15\cdot 31\cdot 8=3720$$

4.4. Ejemplo: Halle todos los números enteros positivos tales que el producto de sus divisores positivos sea 421875.

SOLUCIÓN: Sea n uno cualquiera de tales números. Como es $421875=3^3\cdot 5^6$, el producto de los divisores positivos de n es:

$$n^{\tau\,(n)/2}=3^3\cdot 5^6, \qquad \text{es decir,} \qquad n^{\tau\,(n)}=3^6\cdot 5^{12} \tag{1}$$

por lo que $3^6\cdot 5^{12}$ es potencia $\tau\,(n)$-ésima de un entero positivo, lo que, por ser 3^6 y 5^{12} primos relativos, significa (véase ejemplo 3.7) que 3^6 y 5^{12} son, a su vez, potencias $\tau\,(n)$-ésimas de enteros positivos, es decir, $3^6=a^{\tau\,(n)}$ y $5^{12}=b^{\tau\,(n)}$, donde $a,b\in\mathbb{N}$. Por tanto, $a=3^k$ y $b=5^j$ y entonces $6=k\cdot\tau\,(n)$ y $12=j\cdot\tau\,(n)$, así que $\tau\,(n)$ debe ser divisor de 6. Como es $\tau\,(n)>1$, se da alguna de las posibilidades $\tau\,(n)=2$, $\tau\,(n)=3$ o $\tau\,(n)=6$. No puede ser $\tau\,(n)=2$ porque n no es primo; si fuese $\tau\,(n)=3$, de (1) se deduciría $n=3^2\cdot 5^4$ y entonces $\tau\,(n)=3\cdot 5=15$, imposible; si es $\tau\,(n)=6$, según (1) será

$$n=3\cdot 5^2=75\,,$$

que es la única solución del problema.

4.5. Teorema: *Si el número entero c es múltiplo de los primos relativos a y b, entonces c es múltiplo de ab.*

4.6. Corolario (Múltiplos de un número natural): *Sea* $n = p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r}$ *la factorización canónica del entero positivo* $n > 1$. *Entonces, un número entero* N *es múltiplo de* n *si y sólo si* N *es múltiplo de* $p_i^{k_i}$, *para cada* $i = 1, \dots, r$.

4.7. Ejemplo: Demuestre que $A_n = n^3 - n$ es múltiplo de 24, para todo entero positivo impar n.

SOLUCIÓN: El número entero A_n será múltiplo de $24 = 2^3 \cdot 3 = 8 \cdot 3$ si y sólo si lo es de 8 y de 3. Conviene factorizar A_n, que es:

$$A_n = n(n^2 - 1) = (n-1)n(n+1)$$

- A_n es divisible por 3 por ser el producto de tres números enteros consecutivos, uno de los cuales es múltiplo de 3.
- A_n es divisible por 8, puesto que $n-1$ y $n+1$ son dos pares consecutivos, luego uno de ellos es múltiplo de 2 y el otro múltiplo de 4.

4.8. Cálculo del máximo común divisor y mínimo común múltiplo: *Sean* m *y* n *dos números naturales y* $p_1, p_2, \dots, p_r$ *los distintos números primos que dividen a alguno de los números m o n, de modo que m y n pueden ser escritos en la forma*

$$m = p_1^{j_1} p_2^{j_2} \cdots p_r^{j_r}, \qquad n = p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r},$$

donde $j_i, k_i \geq 0$, *para* $i = 1, \dots, r$. *Entonces,*

$$\text{mcd}(m,n) = p_1^{u_1} p_2^{u_2} \cdots p_r^{u_r}, \qquad \text{mcm}(m,n) = p_1^{v_1} p_2^{v_2} \cdots p_r^{v_r}$$

donde $u_i = \min\{j_i, k_i\}$ *y* $v_i = \max\{j_i, k_i\}$, *para* $i = 1, \dots, r$.

5. Congruencias

5.1. Congruencia módulo n: Sea n un número entero positivo mayor que 1. Se dice que dos números enteros a y b son *congruentes módulo* n, y se escribe $a \equiv b\,(\text{mod}\, n)$, si n es divisor de $a-b$, esto es, si $a-b=kn$, para algún entero k.

5.2. Teorema: *Sean a y b dos números enteros cualesquiera y $n>1$ otro número entero. Entonces, $a \equiv b\,(\text{mod}\, n)$ si y sólo si a y b dan el mismo resto al dividirlos por n.*

DEMOSTRACIÓN: Supongamos que $a \equiv b\,(\text{mod}\, n)$; al dividir los enteros a y b por n, del Algoritmo de la división se deducen $a = nq_1 + r_1$ y $b = nq_2 + r_2$, donde $0 \le r_1, r_2 \le n-1$. Al restar ambas expresiones se deduce que $a-b = n(q_1-q_2)+(r_1-r_2)$, pero como $a-b=kn$, para cierto entero k, al sustituir en la igualdad anterior se deduce que $kn = n(q_1-q_2)+(r_1-r_2)$, es decir, $r_1-r_2 = n(k-q_1+q_2)$ es múltiplo de n, pero como $|\,r_1-r_2\,| \le n-1$, necesariamente $r_1-r_2=0$, es decir, $r_1=r_2$. Si, recíprocamente, a y b dan el mismo resto r al dividirlos por n, se escriben $a = nq_1 + r$, $b = nq_2 + r$, con $0 \le r \le n-1$. Al restar ambas expresiones se deduce: $a-b = n(q_1-q_2)$, y por tanto, $a \equiv b\,(\text{mod}\, n)$ ■

5.3. Corolario: *El número r es el resto de la división del número entero a por el entero positivo n si y sólo si r es el único número entero $r \in \{0,1,\dots,n-1\}$ tal que $a \equiv r\,(\text{mod}\, n)$. En particular, el entero a es divisible por el entero positivo n si y sólo si $a \equiv 0\,(\text{mod}\, n)$.*

5.4. Propiedades de las congruencias: *Sean $n>1$ un número entero y $a,b,c,d \in \mathbb{Z}$. Entonces:*

1. *La congruencia módulo n es una relación de equivalencia, es decir, se trata de una relación reflexiva, simétrica y transitiva.*

2. *La congruencia módulo n es compatible con la suma y el producto en $\mathbb{Z}$, es decir, si $a \equiv b\,(\text{mod}\, n)$ y $c \equiv d\,(\text{mod}\, n)$, entonces*

$$a+c \equiv b+d\,(\text{mod}\, n) \qquad y \qquad ac \equiv bd\,(\text{mod}\, n).$$

3. *Si* $a \equiv b \pmod n$ *y* $p(x) = c_0 + c_1 x + \cdots + c_m x^m$ *es una función polinómica de* x *con coeficientes enteros, entonces* $p(a) \equiv p(b) \pmod n$.

4. *Si* $ca \equiv cb \pmod n$, *entonces* $a \equiv b \left(\operatorname{mod} \frac{n}{d}\right)$, *donde* $d = \operatorname{mcd}(c,n)$.

5. *Si* $ca \equiv cb \pmod n$ *y* $\operatorname{mcd}(c,n) = 1$, *entonces* $a \equiv b \pmod n$.

6. *Si* $ca \equiv cb \pmod p$ *y* $p \nmid c$, *donde* p *es un número primo, entonces* $a \equiv b \pmod p$.

5.5. Ejemplo: ¿Cuál es el resto de dividir 23^{4567} por 12?

SOLUCIÓN: El resto de la división de 23^{4567} por 12 es el único número $r \in \{0,1,2,\ldots,11\}$ tal que $23^{4567} \equiv r \pmod{12}$. Como es $23 \equiv -1 \pmod{12}$, de la propiedad 3 anterior se deduce:

$$23^{4567} \equiv (-1)^{4567} \equiv -1 \equiv 11 \pmod{12}$$

y por tanto el resto de la división es 11.

5.6. Ejemplo: Demuestre que el número $a_n = 3^{2n+2} + 2^{6n+1}$ es divisible por 11, para todo entero no negativo n.

SOLUCIÓN: Debe probarse que $a_n \equiv 0 \pmod{11}$ para cada $n \geq 0$. Esto es fácil, pues

$$a_n = 3^{2n+2} + 2^{6n+1} \equiv 9 \cdot 3^{2n} + 2 \cdot 2^{6n} \equiv 9 \cdot 9^n + 2 \cdot 64^n \equiv 9 \cdot 9^n + 2 \cdot 9^n \equiv (9+2) \cdot 9^n \equiv 11 \cdot 9^n \equiv 0 \pmod{11} \blacksquare$$

5.7. Restos potenciales: Sean b y n dos enteros positivos. Para $i = 0,1,2,\dots$, se llama *i-ésimo resto potencial de b módulo n* al resto r_i que se obtiene al dividir b^i entre n, es decir, r_i es el único número entero $r_i \in \{0,1,\dots,n-1\}$ tal que $b^i = nq_i + r_i$, para algún $q_i \in \mathbb{N}$. Los restos potenciales de b módulo n cumplen las siguientes propiedades:

1. $r_0 = 1$
2. $r_i \equiv b \cdot r_{i-1} \pmod{n}$, *para cada* $i = 1,2,3,\dots$
3. *Si* $r_i = 0$, *entonces* $r_j = 0$ *para cada* $j \geq i$ *(es decir, si un resto potencial es nulo, también lo son todos los siguientes).*
4. *Si existen* $i < j$ *tales que* $r_i = r_j$, *entonces* $r_{i+k} = r_{j+k}$ *para* $k = 0,1,2,\dots$, *es decir, en cuanto se repite un resto, a partir de él se repite toda la secuencia de restos.*

5.8. Ejemplo: Calculamos los restos potenciales de 9 módulo 14.

SOLUCIÓN:

$$9^0 \equiv 1 \pmod{14} \quad \Rightarrow \quad r_0 = 1$$
$$9^1 \equiv 9 \pmod{14} \quad \Rightarrow \quad r_1 = 9$$
$$9^2 \equiv 81 \pmod{14} \equiv 11 \pmod{14} \quad \Rightarrow \quad r_2 = 11$$
$$9^3 \equiv 9 \cdot 11 \pmod{14} \equiv 99 \pmod{14} \equiv 1 \pmod{14} \quad \Rightarrow \quad r_3 = 1$$

Como es $r_3 = r_0$, de la propiedad 4 de los restos potenciales se deduce que para $n = 0,1,2,\dots$ es $r_{3n} = 1$, $r_{3n+1} = 9$, $r_{3n+2} = 11$, esto es,

$$9^{3n} \equiv 1 \pmod{14}, \qquad 9^{3n+1} \equiv 9 \pmod{14}, \qquad 9^{3n+2} \equiv 11 \pmod{14} \quad \blacksquare$$

Los restos potenciales son especialmente útiles en problemas en los que se estudia la divisibilidad de expresiones exponenciales de un número entero por un entero positivo.

5.9. Ejemplo: ¿Cuáles son las dos últimas cifras del número 2107^{2111}?

SOLUCIÓN: Buscamos el único $r \in \{00, 01, \ldots, 99\}$ tal que $2107^{2111} \equiv r \pmod{100}$. De la congruencia $2107 \equiv 7 \pmod{100}$ se desprende que $2107^{2111} \equiv 7^{2111} \pmod{100}$. Dado que

$$7^2 \equiv 49 \pmod{100}, \qquad 7^3 = 343 \equiv 43 \pmod{100}, \qquad 7^4 = 2401 \equiv 1 \pmod{100},$$

resulta, tras dividir 2111 entre 4:

$$2107^{2111} \equiv 7^{2111} \equiv 7^{4\cdot 527+3} = (7^4)^{527} \cdot 7^3 \equiv 1^{527} \cdot 43 \equiv 43 \pmod{100}$$

El número 2107^{2111} termina en las cifras 43.

6. El Pequeño Teorema de Fermat y el Teorema de Wilson

La primera demostración del Pequeño Teorema de Fermat, debida a Euler, no se publicó hasta 1736, casi 100 años después de que Fermat lo postulase. Antes, Leibniz había dejado la misma demostración en un manuscrito de 1683 que nunca se publicó.

6.1. Pequeño Teorema de Fermat: *Sea p un número primo y sea a un número entero que no es múltiplo de p. Entonces:*

$$a^{p-1} \equiv 1 \pmod{p}$$

6.2. Ejemplo: Demuestre que $2^{70}+3^{70}$ es divisible por 13.

SOLUCIÓN: Por el Pequeño Teorema de Fermat, como ni 2 ni 3 son múltiplos de 13, primo, serán $2^{12}\equiv 1(\text{mod}\,13)$ y $3^{12}\equiv 1(\text{mod}\,13)$. Ahora, dado que $70=12\cdot 5+10$:

$$2^{70}+3^{70}\equiv (2^{12})^5\cdot 2^{10}+(3^{12})^5\cdot 3^{10}(\text{mod}\,13)\equiv 2^{10}+3^{10}\,(\text{mod}\,13)\equiv (2^5)^2+(3^3)^3\cdot 3\;(\text{mod}\,13)\equiv 32^2+27^3\cdot 3(\text{mod}\,13)\equiv$$

$$\equiv 6^2+1^3\cdot 3\;(\text{mod}\,13)\equiv 36+3(\text{mod}\,13)\equiv 39(\text{mod}\,13)\equiv 0(\text{mod}\,13)$$

6.3. Corolario: *Si p es un número primo y a es un número entero cualquiera, entonces*

$$a^p\equiv a\,(\text{mod}\,p)$$

DEMOSTRACIÓN: Si a no es divisible por p, del *Pequeño Teorema de Fermat* se deduce que $a^{p-1}\equiv 1(\text{mod}\,p)$ y, tras multiplicar ambos miembros por a, resulta $a^p\equiv a\,(\text{mod}\,p)$. Si a es divisible por p, entonces $a\equiv 0(\text{mod}\,p)$ y por tanto $a^p\equiv 0^p\equiv 0\equiv a\,(\text{mod}\,p)$.

6.4. Ejemplo: Si $p>2$ es un número primo, demuestre que:

a) $1^{p-1}+2^{p-1}+\cdots+(p-1)^{p-1}\equiv -1\;(\text{mod}\,p)$

b) $1^p+2^p+\cdots+(p-1)^p\equiv 0\;(\text{mod}\,p)$

Este problema figura resuelto en la página 59 del volumen Problemas de Matemática Discreta, de E. Bujalance.

SOLUCIÓN: Como ningún $k = 1, \ldots, p-1$ es divisible por el número primo p, según el *Pequeño Teorema de Fermat* 6.1, será $k^{p-1} \equiv 1 \pmod p$, para cualquier $k = 1, \ldots, p-1$. En consecuencia,

$$1^{p-1} + 2^{p-1} + \cdots + (p-1)^{p-1} \equiv 1 + 1 + \overset{p-1}{\cdots} + 1 \equiv p - 1 \equiv -1 \pmod p,$$

Según el Corolario 6.2, $k^p \equiv k \pmod p$, para cada $k = 1, \ldots, p-1$, luego

$$1^p + 2^p + \cdots + (p-1)^p \equiv 1 + 2 + \cdots + (p-1) \equiv \frac{p \cdot (p-1)}{2} \equiv \frac{p-1}{2} \cdot p \equiv 0 \pmod p$$

(repárese, para la última congruencia, en que, por ser $p > 2$ un número primo, p es impar y por tanto $p-1$ es múltiplo de 2) ■

Para concluir estos apuntes, damos una aplicación fundamental de las congruencias lineales llamada Teorema de Wilson, que establece que cualquier primo p es divisor de $(p-1)! + 1$. Este resultado aparece por primera vez en la obra *Meditationes Algebraicae* (1770) del matemático inglés Edward Waring, quien lo conoció gracias a un alumno suyo llamado John Wilson, aunque ninguno de los dos dio demostración alguna del mismo. Fue muy poco después, en 1771, cuando Lagrange publicó una demostración del Teorema de Wilson y de su recíproco, aunque hay evidencias que prueban que Leibniz había formulado y demostrado el citado teorema casi un siglo antes, aunque nunca fue publicado.

6.5. Teorema de Wilson: *Si p es un número primo, entonces*

$$(p-1)! \equiv -1 \pmod p$$

6.6. Ejemplo: Determine el resto de dividir $33!$ por 37.

SOLUCIÓN: Se busca $r \in \{0,1,\ldots,36\}$ tal que $33! \equiv r \pmod{37}$. Dado que 37 es número primo, según el *Teorema de Wilson*:

$$36! \equiv -1 \pmod{37} \quad \Rightarrow \quad 36 \cdot 35 \cdot 34 \cdot 33! \equiv -1 \pmod{37} \quad \Rightarrow \quad (-1)(-2)(-3) \cdot 33! \equiv -1 \pmod{37} \quad \Rightarrow \quad -6 \cdot 33! \equiv -1 \pmod{37} \quad \Rightarrow$$

$$\Rightarrow \quad 6 \cdot 33! \equiv 1 \pmod{37} \quad \Rightarrow \quad 6 \cdot 33! \equiv -36 \pmod{37} \Rightarrow \quad 6 \cdot 33! \equiv 6 \cdot (-6) \pmod{37} \quad \overset{\operatorname{mcd}(6,37)=1}{\Rightarrow} \quad 33! \equiv -6 \pmod{37} \quad \Rightarrow$$

$$\Rightarrow \quad 33! \equiv 31 \pmod{37}$$

El resto de la división de $33!$ por 37 es por tanto 31.

6.7. Observaciones

1. Cuando el entero positivo n es compuesto, obsérvese que si $n = 4$, entonces $(n-1)! = 3! = 6 \equiv 2 \pmod 4$, pero si $n > 4$, entonces n es el producto de dos enteros positivos mayores que 1, alguno de los cuales es mayor que 2, es decir, $n = i \cdot j$, donde $i \le j$, $i \ge 2$ y $j \ge 3$. Si es $i < j$, tanto i como j aparecen en la factorización $1 \cdot 2 \cdot 3 \cdots (n-1)$ de $(n-1)!$, luego $(n-1)!$ es múltiplo de $n = i \cdot j$; si es $i = j$, los números j y $j(j-1)$ están entre los números $3, 4, \ldots, n-1$ y además son distintos pues $3 \le j < j(j-1) < j^2 = n$. Aparece por tanto el factor j al menos dos veces en la factorización $1 \cdot 2 \cdot 3 \cdots (n-1)$, así que $(n-1)!$ es múltiplo de $n = j^2$. Se ha probado así que: *si $n > 4$ es compuesto, entonces $(n-1)!$ es múltiplo de n, es decir,*

$$(n-1)! \equiv 0 \pmod n$$

2. De la observación anterior se deduce que el recíproco del Teorema de Wilson es también cierto, es decir, *si* $(n-1)! \equiv -1 (\text{mod}\, n)$, *entonces* n *es primo.* Así ocurre en efecto, pues si $n = 4$, entonces $3! \equiv 2 \not\equiv -1 (\text{mod}\, 4)$, mientras que si $n > 4$ es compuesto, acaba de probarse que $(n-1)! \equiv 0 \not\equiv -1 (\text{mod}\, n)$.

7. Factorización canónica de $n!$

Recuérdese que la *parte entera* de un número real x, que se escribe $\lfloor x \rfloor$, es el mayor número entero que es menor o igual que x, esto es, $\lfloor x \rfloor$ es el único número entero tal que $x - 1 < \lfloor x \rfloor \leq x$. Es evidente que $\lfloor x \rfloor = x$ si y sólo si x es un número entero. Si n es un entero positivo, el número de veces que aparece un número primo p en la factorización canónica de $n!$ puede expresarse en términos de la función parte entera, como establece el siguiente resultado, que ha sido propuesto un par de veces en las Oposiciones.

7.1. Factorización canónica de $n!$: *Sea n un entero positivo y p un número primo, Entonces:*

1. *p es divisor de $n!$ si y sólo si $p \leq n$.*

2. *Si $p \leq n$, el exponente de p en la factorización canónica de $n!$ es*

$$\sum_{k=1}^{\infty} \left\lfloor \frac{n}{p^k} \right\rfloor,$$

que es una suma finita porque desde cierto k en adelante es $p^k > n$, luego $\left\lfloor \frac{n}{p^k} \right\rfloor = 0$.

Este teorema aparece demostrado de forma distinta a la que aquí se propone en las páginas 580 del volumen 2 y 207 del volumen 3 de la colección de Problemas de Oposiciones de Editorial Deimos.

DEMOSTRACIÓN: Para la prueba de 1 obsérvese que si p es primo y p es divisor de $n!$, entonces $p|k$, para algún $k=2,\dots,n$, luego $p\le k$ y por tanto $p\le n$, Si, recíprocamente, $p\le n$, entonces p es alguno de los factores $1,2,\dots,n$ de $n!$ y por tanto $p\mid n!$. Antes de probar 2, y para mejor entendimiento de lo que se escribirá, calculamos como ejemplo el exponente de $p=2$ en la factorización de $16!$.

$$\begin{array}{cccccccccccccccc}
16!=1\cdot & 2 & \cdot 3\cdot & 4 & \cdot 5\cdot & 6 & \cdot 7\cdot & 8 & \cdot 9\cdot & 10 & \cdot 11\cdot & 12 & \cdot 13\cdot & 14 & \cdot 15\cdot & 16 \\
 & \mathbf{2} & & \mathbf{2}\cdot\mathbf{2} & & \mathbf{2} & & \mathbf{2}\cdot\mathbf{2}\cdot\mathbf{2} & & \mathbf{2} & & \mathbf{2}\cdot\mathbf{2} & & \mathbf{2} & & \mathbf{2}\cdot\mathbf{2}\cdot\mathbf{2}\cdot\mathbf{2}
\end{array}$$

El exponente de 2 en la factorización de $16!$, que es $1+2+1+3+1+2+1+4=15$ puede obtenerse contando de otra manera:

- Número de múltiplos de 2 entre los números 1, 2, 3, … , 16: 8
- Número de múltiplos de 2^2 entre los números 1, 2, 3, … , 16: 4
- Número de múltiplos de 2^3 entre los números 1, 2, 3, … , 16: 2
- Número de múltiplos de 2^4 entre los números 1, 2, 3, … , 16: 1

En total se obtiene 15, que es el exponente de 2 en la factorización de $16!$. Generalizando lo anterior se deduce que el exponente del número primo p $(p\le n)$ en la factorización canónica de $n!$ se obtiene sumando el número de múltiplos de p con el número de múltiplos de p^2, con el número de múltiplos de p^3, … que hay entre los números $1,2,\dots,n$. Pueden contabilizarse como sigue:

- Múltiplos de p entre los números $\{1,2,\dots,n\}$: Entre los primeros n números naturales, aquellos que son divisibles por p son $p,2p,3p,\dots,mp$, donde m es el mayor entero tal que $mp\le n$; en otras palabras, m es el mayor entero menor o igual que $\frac{n}{p}$, es decir, $m=\left\lfloor\frac{n}{p}\right\rfloor$. Así pues, hay exactamente $\left\lfloor\frac{n}{p}\right\rfloor$ múltiplos de p entre los números $1,2,\dots,n$, a saber,

$$p,2p,3p,\dots,\left\lfloor\frac{n}{p}\right\rfloor p \tag{1}$$

- Múltiplos de p^2 entre los números $\{1, 2, \ldots, n\}$: De entre los $\left\lfloor \frac{n}{p} \right\rfloor$ múltiplos de p anteriores, son múltiplos de p^2 los números

$$p^2, 2p^2, 3p^2, \ldots, \left\lfloor \frac{n}{p^2} \right\rfloor p^2$$

  que son, en total, $\left\lfloor \frac{n}{p^2} \right\rfloor$ números.

- Múltiplos de p^3 entre los números $\{1, 2, \ldots, n\}$: Entre los $\left\lfloor \frac{n}{p^2} \right\rfloor$ múltiplos de p^2 anteriores, son múltiplos de p^3 los números

$$p^3, 2p^3, 3p^3, \ldots, \left\lfloor \frac{n}{p^3} \right\rfloor p^3$$

  que son, en total, $\left\lfloor \frac{n}{p^3} \right\rfloor$ números.

Después de un número finito de repeticiones de este proceso, concluimos que el exponente de p primo $(p \le n)$ en la factorización de $n\,!$, esto es, que el total de veces que p divide a $n!$ es

$$\sum_{k=1}^{\infty} \left\lfloor \frac{n}{p^k} \right\rfloor$$

que es una suma finita porque desde cierto $k \in \mathbb{N}$ en adelante es $p^k > n$ y, por tanto, $0 < \frac{n}{p^k} < 1$, así que $\left\lfloor \frac{n}{p^k} \right\rfloor = 0$ ■

7.2. Observaciones

1. Sea cual sea primo p, el exponente del primo p en la factorización canónica de $n!$ es

$$\sum_{k=1}^{\infty} \left\lfloor \frac{n}{p^k} \right\rfloor.$$

En efecto; si $p \leq n$, es lo que establece el Teorema 7.1; si $p > n$, entonces p no divide a $n!$ y el exponente de p en la factorización canónica de $n!$ es cero, que coincide con la suma $\sum_{k=1}^{n} \left\lfloor \frac{n}{p^k} \right\rfloor$, pues para todo $k \geq 1$ es $\left\lfloor \frac{n}{p^k} \right\rfloor = 0$, por ser $n < p \leq p^k$.

2. El resultado 7.1.2 puede reformularse en la siguiente igualdad, llamada *fórmula de Legendre*, que muestra la factorización canónica de $n!$:

$$n! = \prod_{\substack{p \leq n \\ p \text{ primo}}} p^{\sum_{k=1}^{\infty} \left\lfloor \frac{n}{p^k} \right\rfloor}$$

7.3. Ejemplo: Obtenemos la factorización canónica de $40!$

SOLUCIÓN: Los primos divisores de $40!$ son los primos menores o iguales que 40, que son 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31 y 37, y el exponente de cada uno de ellos en la forma canónica de $40!$ es:

- Exponente de 2: $\left\lfloor \frac{40}{2} \right\rfloor + \left\lfloor \frac{40}{4} \right\rfloor + \left\lfloor \frac{40}{8} \right\rfloor + \left\lfloor \frac{40}{16} \right\rfloor + \left\lfloor \frac{40}{32} \right\rfloor = 20 + 10 + 5 + 2 + 1 = 38$
- Exponente de 3: $\left\lfloor \frac{40}{3} \right\rfloor + \left\lfloor \frac{40}{9} \right\rfloor + \left\lfloor \frac{40}{27} \right\rfloor = 13 + 4 + 1 = 18$
- Exponente de 5: $\left\lfloor \frac{40}{5} \right\rfloor + \left\lfloor \frac{40}{25} \right\rfloor = 8 + 1 = 9$
- Exponente de 7: $\left\lfloor \frac{40}{7} \right\rfloor = 5$

- Exponente de 11: $\left\lfloor \frac{40}{11} \right\rfloor = 3$
- Exponente de 13: $\left\lfloor \frac{40}{13} \right\rfloor = 3$
- Exponente de 17: $\left\lfloor \frac{40}{17} \right\rfloor = 2$
- Exponente de 19: $\left\lfloor \frac{40}{19} \right\rfloor = 2$
- Exponente de 23: $\left\lfloor \frac{40}{23} \right\rfloor = 1$
- Exponente de 29: $\left\lfloor \frac{40}{29} \right\rfloor = 1$
- Exponente de 31: $\left\lfloor \frac{40}{31} \right\rfloor = 1$
- Exponente de 37: $\left\lfloor \frac{40}{37} \right\rfloor = 1$

Hemos deducido así que la factorización canónica de $40!$, esto es, su descomposición en factores primos es:

$$40! = 2^{38} \cdot 3^{18} \cdot 5^{9} \cdot 7^{5} \cdot 11^{3} \cdot 13^{3} \cdot 17^{2} \cdot 19^{2} \cdot 23 \cdot 29 \cdot 31 \cdot 37$$