Teoría Elemental de Números

Francisco Javier García Capitán

Problemas del libro *Elementary Number Theory*, de Underwood Dudley.

Índice

1. Enteros

1. **Calcular (314,159) y (4144, 7696)**.

$$\begin{aligned} 314 &= 1 \cdot 159 + 155 \\ 159 &= 1 \cdot 155 + 4 \\ 155 &= 38 \cdot 4 + 3 \\ 4 &= 1 \cdot 3 + 1 \\ 3 &= 3 \cdot 1 \end{aligned}$$

$(314, 159) = (159, 155) = (155, 4) = (4, 3) = (3, 1) = 1.$

$$\begin{aligned} 4144 &= 0 \cdot 7696 + 4144 \\ 7696 &= 1 \cdot 4144 + 3552 \\ 4144 &= 1 \cdot 3552 + 592 \\ 3552 &= 6 \cdot 592 \end{aligned}$$

$(4144, 7696) = (7696, 4144) = (4144, 3552) = (3552, 592) = 592.$

2. **Calcular (3141,1592) y (10001, 1000083)**.

$$\begin{aligned} 3141 &= 1 \cdot 1592 + 1549 \\ 1592 &= 1 \cdot 1549 + 43 \\ 1549 &= 36 \cdot 43 + 1 \\ 43 &= 43 \cdot 1 \end{aligned}$$

$(3141, 1592) = (1592, 1549) = (1549, 43) = (43, 1) = 1.$

$$\begin{aligned} 100083 &= 10 \cdot 10001 + 73 \\ 10001 &= 137 \cdot 73 \end{aligned}$$

$(100083, 10001) = (10001, 73) = 73.$

3. **Encontrar x e y tales que $314x + 159y = 1$.**

$$\begin{gathered} 314 = 1 \cdot 159 + 155 \Rightarrow 155 = 1 \cdot 314 + (-1) \cdot 159 \\ 159 = 1 \cdot 155 + 4 \Rightarrow 4 = (-1) \cdot 314 + 2 \cdot 159 \\ 155 = 38 \cdot 4 + 3 \Rightarrow 3 = 39 \cdot 314 + (-77) \cdot 159 \\ 4 = 1 \cdot 3 + 1 \Rightarrow 1 = (-40) \cdot 314 + 79 \cdot 159 \end{gathered}$$

4. **Encontrar x e y tales que $4144x + 7696y = 1$.**

$$7696 = 1 \cdot 4144 + 3552 \Rightarrow 3552 = 1 \cdot 7696 + (-1) \cdot 4144$$
$$4144 = 1 \cdot 3552 + 592 \Rightarrow 592 = (-1) \cdot 7696 + 2 \cdot 4144$$

5. **Si $N = abc + 1$, demostrar que $(N, a) = (N, b) = (N, c) = 1$.**

   Si d es un divisor positivo de N y de a, entonces también lo será de $N - abc = 1$, por lo que $d = 1$.

6. **Encontrar dos soluciones diferentes de $299x + 247y = 13$.**

   Simplificando por 13, la ecuación es equivalente a $23x + 19y = 1$. Los primeros diez múltiplos de 23 y 19 son:

   23: 23, 46, 69, 92, 115, 138, 161, 184, 207, 230,

   19: 19, 38, 57, 76, 95, 114, 133, 152, 171, 190.

   Observando los números 115 y 114 obtenemos que $23 \cdot 5 + 247 \cdot (-6) = 1$, de donde obtenemos $x = 5, y = -6$. Para encontrar otra solución hallamos otros diez múltiplos de 23 y 19:

   23: 253, 276, 299, 322, 345, 368, 391, 414, 437, 460

   19: 209, 228, 247, 266, 285, 304, 323, 342, 361, 380

   Vemos entonces que $23 \cdot 14 = 322$ y que $19 \cdot 17 = 323$. Por tanto, otra solución sería $x = -14$, $y = 17$.

7. **Demostrar que si $a|b$ y $b|a$ entonces $a = b$ o $a = -b$.**

   Si $a|b$ y $b|a$ entonces existen enteros k y h tales que $b = ka$ y $a = hb$. Si uno de los números a y b es cero, también lo es el otro, y entonces tenemos $a = b$. En otro caso, como $b = ka = khb$, tendremos $kh = 1$, de donde o $k = h = 1$ o $k = h = -1$ que llevan respectivamente a $a = b$ y $a = -b$.

8. **Demostrar que si $a|b$ y $a > 0$, entonces $(a, b) = a$.**

   Que $(a, b) = a$ equivale a decir que $a|a$, $a|b$ y que si $c|a$ y $c|b$, entonces $c \leq a$. Que $a|a$ es evidente, que $a|b$ es una de las hipótesis y, por último, de $c|a$ deducimos que $a = kc$ para algún entero k, y como $a > 0$, deducimos que $c \leq a$.

9. **Demostrar que si** $((a,b),b) = (a,b)$.

   Podemos usar el ejercicio anterior y tener en cuenta que $(a,b)|b$ y $(a,b) > 0$. Por tanto, $((a,b),b) = (a,b)$.

10. *a)* **Demostrar que** $(n, n+1) = 1$ **para todo** $n > 1$.

    b) **Si** $n > 0$**, ¿cuánto puede valer** $(n, n+2)$**?**

    a) Sea d un divisor positivo de n y $n+1$. Entonces también lo será de $(n+1) - n = 1$, por lo que $d = 1$.

    b) Sea d un divisor positivo de n y $n+2$. Entonces también lo será de $(n+2) - n = 2$, por lo que $d = 1$ ó $d = 2$.

11. *a)* **Demostrar que** $(k, n+k) = 1$ **si y solo si** $(k,n) = 1$.

    b) **¿Es cierto que** $(k, n+k) = d$ **si y solo si** $(k,n) = d$**?**

    a) Supongamos que $(k, n+k) = 1$ y sea d un divisor positivo de n y k. Entonces podremos expresar $k = du$, $n = dv$ y $k + n = du + dv = d(u+v)$, por lo que d es un divisor positivo de k y $n+k$ y debe ser 1. Recíprocamente y de forma análoga, si suponemos que $(k,n) = 1$ y d es un divisor positivo de k y $n+k$, tendremos $k = du$, $n + k = dv$, por lo que $n = (n+k) - k = d(v-u)$ y obtenemos que d es un divisor positivo de k y n. Por ello, como $(k,n) = 1$, debe ser $d = 1$ y también $(k, n+l) = 1$.

    b) Sí, es cierto. Sean $(k, n+k) = d$ y $(k,n) = e$. e es un divisor de n y k. Entonces podremos expresar $k = eu$, $n = ev$ y $k + n = eu + ev = e(u+v)$, por lo que e es un divisor de k y $n+k$ y debe ser $e|d$. De forma parecida, al ser d un divisor común de k y $n+k$ podremos escribir $k = du$ y $n + k = dv$ lo que permite escribir $n = d(v-u)$ siendo entonces d un divisor de k y n. Por tanto $d|e$. Como $d|e$ y $e|d$, y ambos son positivos, $d = e$.

12. **Demostrar que si** $a|b$ **y** $c|d$**, entonces** $ac|bd$.

    Expresemos $b = ka$ y $d = hc$ y tendremos $bd = (ka)(hc) = (kh)(ac)$, de donde $ac|bd$.

13. **Demostrar que si** $d|a$ **y** $d|b$**, entonces** $d^2|ab$.

    Expresemos $a = kd$ y $b = hd$ y tendremos $ab = (kd)(hd) = (kh)d^2$, de donde $d^2|ab$.

14. **Demostrar que si $c|ab$ y $(c,a)=d$, entonces $c|db$.**

Como $c|ab$, existe un entero k tal que $ab=kc$ y como $(c,a)=d$, existen enteros x e y tales que $cx+ay=d$. Multiplicando esta última igualdad por b, tenemos que $db=bcx+aby=bcx+kcy=c(bx+ky)$, por lo que $c|db$.

15. *a)* **Demostrar que si $x^2+ax+b=0$ tiene una raíz entera, es un divisor de b.**

b) **Demostrar que si $x^2+ax+b=0$ tiene una raíz racional, es en realidad un número entero**.

a) Sea m una raíz entera de $x^2+ax+b=0$. Entonces $b=-m^2-am=m(-m-a)$. Por tanto, m debe ser un divisor de b.

b) Sea $\frac{p}{q}$ una raíz racional irreducible de $x^2+ax+b=0$. Entonces

$$\frac{p^2}{q^2}+b\frac{p}{q}+c=0 \Rightarrow p^2+bpq+cq^2=0 \Rightarrow p^2=-q(bp+cq).$$

Como la fracción $\frac{p}{q}$ es irreducible y q es un divisor de p^2, también lo es de p. En efecto, de $p^2=qh$ y $px+qy=1$, podemos obtener $p^2x+pqy=p$ y $qhx+pqy=p$, y entonces $p=q(hx+qy)$. Por tanto $q=1$ y la fracción $\frac{p}{q}$ es un entero.

2. Factorización única

1. **Desomponer factorialmente 1234, 34560 y 111111**.

   $1234 = 2 \cdot 617$, $34560 = 2^8 \cdot 3^3 \cdot 5$, $111111 = 3 \cdot 7 \cdot 11 \cdot 13 \cdot 37$.

2. **Descomponer factorialmente de 2345, 45670 y 999999999999. (Observar que** $101|1000001$**)**.

   $2345 = 5 \cdot 7 \cdot 67$. $45670 = 2 \cdot 5 \cdot 4567$.

   $999999999999 = 3^3 \cdot 7 \cdot 11 \cdot 13 \cdot 37 \cdot 101 \cdot 9901$.

3. **Tartaglia (1556) afirmaba que las sumas** $1+2+4$, $1+2+4+8$, $1+2+4+8+16$, **... eran alternadamente números primos y compuestos. Demostrar que estaba equivocado**.

   Teniendo en cuenta que $1+2+4+\cdots+2^{n-1} = 2^n - 1$, construimos la tabla

n	3	4	5	6	7	8	9
$2^n - 1$	7	15	31	63	127	255	511
¿Primo?	SI	NO	SI	NO	SI	NO	NO

   Vemos que a $511 = 7 \cdot 73$ le tocaría ser primo y no lo es.

4. *a*) **DeBouvelles (1509) afirmaba que para cada** $n \geq 1$ **uno o ambos de los números** $6n+1$ **y** $6n-1$ **son primos. Demostrar que estaba equivocado**.

   b) **Demostrar que hay infinitos números** n **tales que tanto** $6n+1$ **como** $6n-1$ **son compuestos**.

   a) Si introducimos en *Mathematica* la instruccción

   ```
   Table[{PrimeQ[6*n+1], PrimeQ[6*n-1]}, {n,1,20}],
   ```

   obtenemos que $n = 20$ es el primer valor para el que $6n+1 = 121 = 11^2$ y $6n-1 = 7 \cdot 119$ son ambos compuestos.

   b) Sea n cualquier número de la forma $n = 77k - 57$. Entonces:

$$6n + 1 = 462k - 342 + 1 = 462k - 341 = 11(42k - 31)$$
$$6n - 1 = 462k - 342 - 1 = 462k - 343 = 7(66k - 49)$$

(La solución a este apartado la encontré buscando los números compuestos de la forma $6n+1$ y $6n-1$ divisibles por 11 uno y por 7 otro, y encontrando que se van diferenciando 77 unos de otros).

5. **Demostrar que los exponentes en la descomposición factorial de un cuadrado perfecto son pares**.

   Si $n = m^2$ y $m = p_1^{e_1} p_2^{e_2} \cdots p_r^{e_r}$, obtenemos que $n = (p_1^{e_1} p_2^{e_2} \cdots p_r^{e_r})^2 = p_1^{2e_1} p_2^{2e_2} \cdots p_r^{2e_r}$.

6. **Demostrar que si los exponentes en la descomposición factorial de un número son pares, dicho número es cuadrado perfecto**.

   Supongamos que n tiene una descomposición factorial de la forma $n = p_1^{2e_1} p_2^{2e_2} \cdots p_r^{2e_r}$. Entonces $n = (p_1^{e_1} p_2^{e_2} \cdots p_r^{e_r})^2 = m^2$, siendo $m = p_1^{e_1} p_2^{e_2} \cdots p_r^{e_r}$.

7. **Encontrar el entero más pequeño divisible por 2 y 3 que es a la vez un cuadrado y una quinta potencia**.

   Cualquier número de la forma $n = 2^{10k} 3^{10h}$, con $h, k \geq 1$ es divisible por 2 y por 3, y es un cuadrado y una quinta potencia. Para $k = 1$ y $h = 1$, resulta $n = 6^{10} = 60466176$.

8. **Si $d|ab$, ¿se deduce que $d|a$ o $d|b$?**

   No, pues, por ejemplo, $12|36$, pero ni $12|9$, ni $12|4$.

9. **¿Es posible que un primo p divida tanto a n como a $n+1$ ($n \geq 1$).**

   No pues también dividiría a $(n+1) - n = 1$.

10. **Demostrar que $n(n+1)$ nunca es un cuadrado para $n > 0$.**

    Sean $m, n > 0$ tales que $n^2 + n = m^2$. Resulta $n = m^2 - n^2 = (m+n)(m-n)$. Por tanto, $m + n \leq n \Rightarrow m \leq 0$. Contradicción.

11. *a)* **Comprobar que $2^5 \cdot 9^2 = 2592$.**

    b) **¿Es $2^5 \cdot a^b = 25ab$ posible para otros a, b? (Aquí $25ab$ representa los dígitos de $2^5 \cdot a^b$, no un producto.)**

    a) $2^5 \cdot 9^2 = 32 \cdot 81 = 2592$.

b) Escribiendo el la igualdad propuesta en la forma

$$a^b = \frac{2500 + ab}{32} = 78{,}125 + \frac{ab}{32},$$

y teniendo en cuenta que ab puede ser como mucho 98, llegamos a $78 < a^b \leq 78{,}125 + \frac{98}{32} = 78{,}125 + 3{,}0625 = 81{,}1875$. Es decir, a^b sólo puede ser 79, 80 u 81. Sólo 81 es una potencia de un número entero. Además, lo es de dos formas, 9^2 y 3^4. La solución $a = 3, b = 4$ no es válida pues el valor de a^b es único y sólo coincide con la solución $a = 9, b = 2$.

12. **Sea p el factor primo menor de n, siendo n compuesto. Demostrar que si $p > n^{1/3}$, entonces n/p es primo**.

Razonamos por reducción al absurdo. Supongamos que n/p no es primo. Entonces existe un primo q que divide propiamente a n/p, es decir cumple que $pq < n$. El número n/pq o es un primo r o es divisible por un primo r que también divide a n. En cualquier caso, tenemos $pqr \leq n$, en contradicción con que, al ser p el menor de los primos que dividen a n, $pqr \geq p^3 > n$.

13. **¿Verdadero o falso? Si p y q dividen a n, y ambos son mayores que $n^{1/4}$, entonces n/pq es primo**.

Consideramos $p = 5$ y $q = 7$ y $n = 6pq = 210$. Tanto p como q son mayores que $n^{1/4}$, y sin embargo $n/pq = 6$ no es primo.

14. **Demostrar que si n es compuesto, entonces $2^n - 1$ es compuesto**.

Supongamos que $n = pq$. Sustituyendo $b = 2^p$ y $a = 1$ en la fórmula

$$b^q - a^q = (b - a)(b^{q-1} + ab^{q-2} + \cdots + a^{q-2}b + a^{q-1})$$

obtenemos

$$2^n - 1 = (2^p - 1)(2^{p(q-1)} + 2^{p(q-2)} + \cdots + 2^p + 1),$$

por lo que $2^n - 1$ es compuesto.

15. **¿Es cierto que si $2^n - 1$ es compuesto, entonces n es compuesto?**

No es cierto, puesto que $2^{11} - 1 = 2047 = 23 \cdot 89$ es compuesto, mientras que 11 es primo.

3. Ecuaciones diofánticas lineales

1. **Encontrar todas las soluciones enteras de** $x+y=2$**,** $3x-4y=5$ **y** $15x+16y=17$.

   Es fácil encontrar una solución de cada una de las ecuaciones: $x=1, y=1$, para la primera, $x=3, y=1$ para la segunda y $x=-17, y=17$ para la tercera. Entonces, las soluciones de estas ecuaciones vendrán dadas por las fórmulas:

$$\begin{cases} x=1+t \\ y=1-t \end{cases}, \quad \begin{cases} x=3-4t \\ y=1-3t \end{cases}, \quad \begin{cases} x=-17+16t \\ y=17-15t \end{cases}.$$

2. **Encontrar todas las soluciones enteras de** $2x+y=2$**,** $3x-4y=0$ **y** $15x+18y=17$.

   La última ecuación no tiene ninguna solución, pues $(15,18)=3$ no es un divisor de 17. Una solución de la primera es $x=1, y=0$ y una solución de la segunda es $x=0, y=0$. Entonces, las soluciones de estas ecuaciones son:

$$\begin{cases} x=1+t \\ y=-2t \end{cases}, \quad \begin{cases} x=-4t \\ y=-3t \end{cases}.$$

3. **Encontrar todas las soluciones enteras positivas de** $x+y=2$**,** $3x-4y=5$ **y** $6x+15y=51$.

   Las soluciones enteras de $x+y=2$ son de la forma $x=1-t$, $y=1+t$. Para que x e y sean positivos, t debe cumplir las desigualdades $t<1$ y $t>-1$. Sólo puede ser $t=0$ y entonces la única solución positiva de esta ecuación es $x=1$, $y=1$.

   Las soluciones enteras de $3x-4y=5$ son de la forma $x=3-4t$, $y=1-3t$. Para que x e y sean positivos, t debe cumplir las desigualdades $t<\frac{4}{3}$ y $t<\frac{1}{3}$, que se cumplen ambas si y solo si $t\leq 0$. Por tanto las soluciones enteras positivas de $3x-4y=5$ las podemos expresar así:

$$\begin{cases} x=3+4t \\ y=1+3t \end{cases}, \ (t\geq 0).$$

Las soluciones enteras de $6x + 15y = 51$ son las mismas que las de $2x + 5y = 17$ y una de ellas es $x = 1, y = 3$. Las demás son de la forma

$$\begin{cases} x = 1 + 5t \\ y = 3 - 3t \end{cases}.$$

Para que x e y sean positivos es necesario que $t \geq 0$ y $t < 1$, es decir, el único valor de t posible es $t = 0$ y la única solución positiva es $x = 1$, $y = 3$.

4. **Encontrar todas las soluciones positivos de** $2x+y = 2$**,** $3x-4y = 0$ **y** $7x + 15y = 51$.

   Empezamos por hallar las soluciones enteras de estas ecuaciones:

$$\begin{cases} x = t \\ y = 2 - 2t \end{cases}, \quad \begin{cases} x = 4t \\ y = 3t \end{cases}, \quad \begin{cases} x = -102 + 15t \\ y = 51 - 7t \end{cases}.$$

   Ahora es fácil encontrar los valores de t que hacen que x e y sean positivos. En el primer caso no hay ningún valor de t. En el segundo caso es válido cualquier $t \geq 1$. En la tercera ecuación, debe ser $\frac{102}{15} < t < \frac{51}{7}$ ó $6{,}8 < t < 7\frac{2}{7}$, es decir debe ser $t = 7$, que da lugar a $x = 3, y = 2$ como única solución positiva.

5. **Encontrar todas las soluciones positivas de**

$$\begin{cases} x + y + z = 31 \\ x + 2y + 3z = 41 \end{cases}$$

   Restando las dos ecuaciones, obtenemos $y + 2z = 10$, cuyas soluciones son de la forma

$$\begin{cases} y = 2t \\ z = 5 - t \end{cases},$$

   que nos lleva a $x = 31 - 2t - (5 - t) = 26 - t$. Para que x, y, z sean positivos, debe ser $t > 0$, $t < 54$ y $t < 26$, es decir $t = 1, 2, 3, 4$ que dan lugar a las soluciones

t	1	2	3	4
x	25	24	23	22
y	2	4	6	8
z	4	3	2	1

6. **Encuentra las cinco formas diferentes de sumar $4.99 con 100 monedas de 1, 10 y 25 centavos**.

   Planteamos el problema con el sistema

$$\begin{cases} x + y + z = 100 \\ x + 10y + 25z = 499 \end{cases}.$$

   Restando las dos ecuaciones obtenemos $9y + 24z = 399$, y dividiendo por 3, $3y + 8z = 133$. Para resolver esta ecuación, despejamos:

$$y = \frac{133 - 8z}{3} = 44 - 2z + \frac{1 - 2z}{3} = 44 - 2z + p,$$

   cumpliendo p que $3p + 2z = 1$, y de nuevo despejando,

$$z = \frac{1 - 3p}{2} = \frac{1 - p}{2} - p = q - p,$$

   donde $1 - p = 2q$, y por tanto, $p = 1 - 2q$. Ahora, vamos sustituyendo y obteniendo $z = q - p = q - (1 - 2q) = 3q - q$, $y = 44 - 2z + p = 44 - 2(3q - 1) + (1 - 2q) = 47 - 8q$, $x = 100 - y - z = 100 - (47 - 8q) - (3q - 1) = 54 + 5q$. Como x, y, z deben ser no negativos, $q \leq 1$ y $q \leq 5$, que da lugar a los siguientes valores de x, y, z:

q	1	2	3	4	5
x	59	64	69	74	79
y	39	31	23	15	7
z	2	5	8	11	14

7. **Un hombre compró doce piezas de fruta (manzanas y naranjas) por 99 centavos. Si una manzana cuesta 3 céntimos más que una naranja, y compró más manzanas que naranjas, ¿cuántas de cada compró?**

   Llamamos x, y al número de manzanas y peras, respectivamente, y p al precio de una naranja. Entonces

$$\begin{cases} x + y = 12 \\ (p + 3)x + py = 99 \end{cases} \Rightarrow \begin{cases} x + y = 12 \\ 3x + p(x + y) = 99 \end{cases} \Rightarrow \begin{array}{c} 3x + 12p = 99 \\ x + 3p = 33 \\ x = 33 - 3p \end{array}.$$

Sustituyendo, $y = 12 - x = 12 - (33 - 4p) = 4p - 21$. Como compró más manzanas que naranjas, $33 - 4p > 4p - 21 \Rightarrow 54 > 8p \Rightarrow p \leq 6$. Por otro lado, x e y deben ser positivos, por lo que $4p - 21 \leq 0 \Rightarrow p \geq 6$. Sólo puede ser $p = 6$, que da $x = 9$ manzanas e $y = 3$ naranjas.

8. **En una clase de teoría de números hay estudiantes de segundo, tercer y cuarto curso. Si cada estudiante de segundo curso contribuye con \$1.25, cada uno de tercero con \$0.90 y cada uno de cuarto con \$0.50, el instructor recibirá una paga de \$25. Hay 26 estudiantes; ¿cuántos hay de cada?**

   Llamando x, y, z al número de alumnos de segundo, tercer y cuarto curso, respectivamente, planteamos el sistema

$$\begin{cases} x + y + z = 26 \\ 125x + 90y + 50z = 2500 \end{cases} \Rightarrow \begin{cases} x + y + z = 26 \\ 25x + 18y + 10z = 500 \end{cases}.$$

   Multiplicando por 10 la primera ecuación y restándosela a la segunda obtenemos $15x + 8y = 240$. Teniendo en cuenta que $8 \cdot 15 = 120$, hallamos que $x = 8$, $y = 15$ es una solución entera de esta última ecuación, por lo que todas las otras serán de la forma

$$\begin{cases} x = 8 + 8t \\ y = 15 - 15t \end{cases},$$

   , y entonces $z = 26 - x - y = 26 - (8 + 8t) - (15 - 15t) = 3 + 7t$. Evidentemente, la única solución positiva se obtiene para $t = 0$: 8 alumnos de segundo curso, 15 de tercero y 3 de cuarto.

9. **El siguiente problema apareció por primera vez en un libro indio escrito sobre el año 850. Tres mercaderes encontraron una bolsa en el camino. Uno de ellos dijo: "Si yo consigo esta bolsa, seré el doble de rico que vosotros dos juntos". Entonces el segundo dijo: "Yo seré el doble de rico que vosotros juntos". El tercer hombre dijo: "Yo seré tan rico como cinco veces vosotros dos juntos". ¿Cuánto tenía cada mercader y cuánto había en la bolsa?**

   Sean x, y, z la cantidad poseída por los tres mercaderes y b la cantidad

que contiene la bolsa. Entonces:

$$\begin{cases} x+b=2(y+z) \\ y+b=3(x+z) \\ z+b=5(x+y) \end{cases} \Rightarrow \begin{cases} x=2y+2z-b \\ y+b=3x+3z \\ z+b=5x+5y \end{cases} \Rightarrow \begin{cases} y+b=6y+9z-3b \\ z+b=15y+10z-5b \end{cases}$$

$$\begin{cases} 5y+9z=4b \\ 15y+9z=6b \end{cases} \Rightarrow 10y=2b \Rightarrow y=\frac{b}{5} \Rightarrow 9z=3b \Rightarrow z=\frac{b}{3}.$$

Finalmente, $x=\left(\frac{2}{5}+\frac{2}{3}-1\right)b=\frac{b}{15}$.

10. **Un hombre cobra un cheque por d dólares y c centavos en un banco. El cajero, por error, le da c dólares y d centavos. El hombre no se da cuenta hasta que gasta 23 centavos y además se da cuenta que en ese momento tiene $2d$ dólares y $2c$ centavos. ¿Cuál era el valor del cheque?**

Planteemos la ecuación $(100c+d)-23=200d+2c$ y obtendremos $98c-199d=23$. Usemos el algoritmo de Euclides para encontrar una solución de esta ecuación:

$$\begin{array}{ll} 199=2\cdot 98+3 & 3=(-2)\cdot 98+1\cdot 199 \\ 98=32\cdot 3+2 & 2=65\cdot 98+(-32)\cdot 199 \\ 3=1\cdot 2+1 & 1=(-67)\cdot 98+33\cdot 199 \end{array}$$

Entonces $c=-67$, $d=-33$ es una solución de $98c-199d=1$ y, multiplicando por 23, $c=-1541$, $d=-759$ es una solución de $98c-199d=23$. Las demás soluciones serán de la forma

$$\begin{cases} c=-1541+199t \\ d=-759+98t \end{cases}.$$

Para $t\geq 8$ es cuando se obtienen valores positivos de c y d: Para $t=8$, $c=51$, $d=25$. Para valores mayores de t, c sería mayor que 100, que es imposible. Por tanto, el valor del cheque era de 25 dólares y 51 centavos.

4. Congruencias

1. **Encontrar el resto de 1492 (mód 4), (mód 10) y (mód 101).**

   Dividiendo 1492 por 4, 10 y 101 obtenemos de resto 0, 2 y 78 respectivamente. Entonces:

   $1492 \equiv 0$ (mód 4), $1492 \equiv 2$ (mód 10) y $1492 \equiv 78$ (mód 101).

2. **Encontrar el resto de 1789 (mód 4), (mód 10) y (mód 101).**

   Dividiendo 1789 por 4, 10 y 101 obtenemos de resto 1, 9 y 72, respectivamente. Entonces:

   $1789 \equiv 1$ (mód 4), $1789 \equiv 9$ (mód 10) y $1789 \equiv 72$ (mód 101).

3. **¿Es cierto que $a \equiv b$ (mód m), implica que $a^2 \equiv b^2$ (mód m).**

   Es cierto, pues si $a \equiv b$ (mód m), m es un divisor de $a - b$, por lo que también lo será de $(a - b)(a + b) = a^2 - b^2$.

4. **¿Es cierto que $a^2 \equiv b^2$ (mód m), implica que $a \equiv b$ (mód m).**

   En principio, todo divisor de $a^2 - b^2$ no tiene por qué serlo de $a - b$. Por ejemplo, para $a = 7$ y $b = 5$, $a^2 - b^2 = 49 - 24 = 24$. Basta tomar $m = 3$, para tener $49 \equiv 25 \equiv 1$ (mód 3) y sin embargo, $7 \equiv 1$ (mód 3) y $5 \equiv 2$ (mód 3)

5. **Encontrar todos los m tales que $1066 \equiv 1776$ (mód m).**

   m deberá ser un divisor de $710 = 1776 - 1066$. Como $710 = 2 \cdot 5 \cdot 71$, los divisores de 710 son 1, 2, 5, 10, 71, 142, 355 y 710.

6. **Encontrar todos los m tales que $1848 \equiv 1914$ (mód m).**

   m deberá ser un divisor de $66 = 1914 - 1848$. Como $66 = 2 \cdot 3 \cdot 11$, los divisores de 66 son 1, 2, 3, 6, 11, 22, 33, 66.

7. **Si $k \equiv 1$ (mód 4), con quién es congruente $6k + 5$ (mód 4)?**

   Si escribimos $k = 1 + 4m$, $6k + 5 = (6 + 24m) + 5 = 24m + 11 \equiv 3$ (mód m).

8. **Demostrar que todos los primos (excepto el 2) es congruente con 1 ó 3 módulo 4.**

   Los restos módulo 4 son 0, 1, 2, 3. Aquellos números que dan resto módulo 0 o 2 son pares, y no pueden ser primos.

9. **Demostrar que todos los primos (excepto el 2 y el 3) son congruentes con 1 ó 5 módulo 6**.

   Los restos módulo 6 son 0, 1, 2, 3, 4, 5. Aquellos números que dan resto módulo 0, 2 o 4 son pares, y no pueden ser primos y los dan resto módulo 3, son de la forma $6k + 3 = 3(2k + 1)$, es decir, son divisibles por 3, y tampoco pueden ser primos.

10. **¿Con qué pueden ser congruentes módulo 30 los primos distintos de 2, 3 o 5?**

    Quitaremos de los números, {0,1,...,29}, los pares mayores que 2, los múltiplos de 3 mayores que 3, los múltiplos de 5 mayores que 5, etc. Quedarán 1,7,11,13,17,19,23,29.

11. **En la multiplicación** $314159 \cdot 92653 = 2910\,93995$**, se ha perdido un dígito del producto y todos los demás son correctos. Encontrar el dígito perdido sin efectuar la multiplicación**.

    Usamos la prueba del nueve, basada en las congruencias módulo 9. Al sumar las cifras de 314159 y 92653 obtenemos 5 y 7 módulo 9, respectivamente. La suma de cifras del producto debe ser congruente con 35 módulo 9, es decir 8 módulo 9. Como la suma de cifras del producto es 2 módulo 9, la cifra que falta es un 6.

12. **Demostrar que ningún cuadrado tiene como último dígito 2, 3, 7 u 8**.

    Basta hacer congruencias módulo 10, o lo que es lo mismo fijarse en u, la cifra de las unidades cuando elevamos al cuadrado los números n del 0 al 9.

n	0	1	2	3	4	5	6	7	8	9
u	0	1	4	9	6	5	6	9	4	1

13. **¿Cuál puede ser el último dígito de una cuarta potencia**.

    De forma parecida al ejercicio anterior, nos podemos fijar en u, la cifras de las unidades cuando elevamos al cuadrado uno de los números $n = 0, 1, 4, 5, 6, 9$:

n	0	1	4	5	6	9
u	0	1	6	4	6	1

Por tanto, el último dígito de una cuarta potencia puede ser 0, 1, 4 o 6.

14. **Demostrar que la diferencia de dos cubos consecutivos nunca es divisible por 3**.

Basta tener en cuenta que $(n+1)^3 - n^3 = 3n^2 + 3n^2 + 1$ da de resto 1 módulo 3.

15. **Demostrar que la diferencia de dos cubos consecutivos nunca es divisible por 5**.

Dando a la expresión $3n^2 + 3n + 1$ los valores 0, 1, 2, 3, 4 obtenemos, respectivamente, 1, 7, 19, 37, 61, y ninguno de estos números es divisible por 5.

16. **Demostrar que**

$$\begin{aligned} &d_k 10^k + d_{k-1}10^{k-1} + \cdots + d_1 10 + d_0 \\ &\equiv d_0 - d_1 + d_2 - d_3 + \cdots + (-1)^k d_k \pmod{11} \end{aligned}$$

y deducir un criterio de divisibilidad por 11.

Para demostrar esta fórmula es suficiente comprobar que si n es par entonces $10^n \equiv (-1)^{n+1} \pmod{11}$ y ello se deduce fácilmente por inducción de que $10^1 \equiv -1 \pmod{11}$ y que $10^2 \equiv 1 \pmod{11}$ y por tanto,

$$\begin{aligned} &d_k 10^k + d_{k-1}10^{k-1} + \cdots + d_1 10 + d_0 \\ &\equiv d_0 + d_1(-1) + d_2 + d_3(-1) + \cdots + (-1)^k d_k \pmod{11} \\ &\equiv d_0 - d_1 + d_2 - d_3 + \cdots + (-1)^k d_k \pmod{11} \end{aligned}$$

17. **A dice que 27,182,818,284,590,452 es divisible por 11. B dice que no. ¿Quién lleva razón?**

Usando el criterio encontrado en el ejercicio anterior, cuando un número sea divisible por 11, también lo será la diferencia de las sumas de los dígitos que ocupan posiciones impares y pares del número. En nuestro caso, los dígitos que ocupan posiciones impares suman $2+1+2+1+2+4+9+4+2 = 27$ y los que ocupan posiciones impares, $7+8+8+8+5+0+5 = 49$. La diferencia es $49 - 27 = 22$, que es divisible por 11. Por tanto, A tiene razón.

18. **Un *palíndromo* es un número que se lee igual hacia delante y hacia detrás. Por ejemplo, 22, 1331 y 935686539 son palíndromos.**

   a) **Demostrar que todo palíndromo de 4 dígitos es divisible por 11**.

   b) **¿Qué ocurre con los palíndromos de seis dígitos?**

   a) **Aplicamos el criterio visto en el ejercicio 16. Si** $N = abba$**, será** $a - b + b - a = 0$ **por lo que** N **es divisible por 11**.

   b) **Si** $N = abccba$**,** N **es congruente módulo 11 con** $a - b + c - c + b - a = 0$**, por lo que también será divisible por 11**.

19. **Demostrar que si** $n \equiv 4$ **(mód 9), entonces** n **no puede escribirse como suma de tres cubos**.

   Ponemos en una tabla los valores de k, k^2 y k^3 módulo 9, dando a n los valores de los restos módulo 9:

k	0	1	2	3	4	5	6	7	8
k^2	0	1	4	0	7	7	0	4	1
k^3	0	1	8	0	1	8	0	1	8

   Vemos que los valores posibles de k^3 son 0, 1 y 8. Al sumar tres números que sean 0, 1 u 8, módulo 9, los resultados posibles son $0+0+0=0$, $0+0+1=1$, $0+0+8=8$, $0+1+1=2$, $0+1+8=0$, $0+8+8=7$, $1+1+1=3$, $1+1+8=1$, $1+8+8=8$ y $8+8+8=6$, así que nos posible obtener un número que sea congruente con 4 módulo 9 como suma de tres cubos. (Tampoco uno que sea congruente con 5 módulo 9).

20. **Demostrar que para cualquiera** $k > 0$ **y** $m \geq 1$**,** $x \equiv 1$ **(mód** m^k**) implica que** $x^m \equiv 1$ **(mód** m^{k+1}**)**.

   Que $x \equiv 1 \pmod{m^k}$ significa que $x = 1 + ym^k$ siendo y un número entero. Usamos la fórmula del binomio:

$$x^m = (1 + ym^k)^m = 1 + \binom{m}{1} ym^k + \binom{m}{2} (ym^k)^2 + \cdots + (y^m k)^m$$

   Como todos los sumandos, excepto el primero son divisibles por m^{k+1}, resulta que $x^m \equiv 1 \pmod{m^{k+1}}$.

5. Congruencias lineales

1. **Resolver las siguientes congruencias**:

$$2x \equiv 1 \text{ (mód 17)} \quad 3x \equiv 1 \text{ (mód 17)}$$
$$3x \equiv 6 \text{ (mód 18)} \quad 40x \equiv 777 \text{ (mód 1777)}$$

$2x \equiv 1 \text{ (mód 17)} \Leftrightarrow 2x \equiv 18 \text{ (mód 17)} \Leftrightarrow x \equiv 9 \text{ (mód 17)}.$

$3x \equiv 1 \text{ (mód 17)} \Leftrightarrow 3x \equiv 18 \text{ (mód 17)} \Leftrightarrow x \equiv 6 \text{ (mód 17)}.$

$3x \equiv 6 \text{ (mód 18)} \Leftrightarrow x \equiv 2 \text{ (mód 6)} \Leftrightarrow x \equiv 2, 8, 14 \text{ (mód 18)}.$

$40x \equiv 777 \text{ (mód 1777)} \Leftrightarrow 40x \equiv -1000 \text{ (mód 1777)} \Leftrightarrow$
$\Leftrightarrow x \equiv -25 \text{ (mód 1777)} \Leftrightarrow x \equiv 1752 \text{ (mód 1777)}.$

2. **Resolver las siguientes congruencias**:

$$2x \equiv 1 \text{ (mód 19)} \quad 3x \equiv 1 \text{ (mód 19)}$$
$$4x \equiv 6 \text{ (mód 18)} \quad 20x \equiv 984 \text{ (mód 1984)}$$

$2x \equiv 1 \text{ (mód 19)} \Leftrightarrow 2x \equiv 20 \text{ (mód 19)} \Leftrightarrow x \equiv 10 \text{ (mód 19)}.$

$3x \equiv 1 \text{ (mód 19)} \Leftrightarrow 3x \equiv 39 \text{ (mód 19)} \Leftrightarrow x \equiv 13 \text{ (mód 19)}.$

$4x \equiv 6 \text{ (mód 18)} \Leftrightarrow 4x \equiv 24 \text{ (mód 18)} \Leftrightarrow$
$\Leftrightarrow x \equiv 6 \text{ (mód 9)} \Leftrightarrow x \equiv 6, 15 \text{ (mód 18)}.$

$20x \equiv 984 \text{ (mód 1984)} \Leftrightarrow 20x \equiv -1000 \text{ (mód 1984)} \Leftrightarrow$
$\Leftrightarrow x \equiv -50 \text{ (mód 496)} \Leftrightarrow x \equiv 446 \text{ (mód 496)} \Leftrightarrow$
$\Leftrightarrow x \equiv 446, 992 \text{ (mód 1984)}.$

3. **Resolver los sistemas**

a) $x \equiv 1 \text{ (mód 2)}, x \equiv 1 \text{ (mód 3)}.$

b) $x \equiv 3 \text{ (mód 5)}, x \equiv 5 \text{ (mód 7)}, x \equiv 7 \text{ (mód 11)}.$

c) $2x \equiv 1 \text{ (mód 5)}, 3x \equiv 2 \text{ (mód 7)}, 4x \equiv 3 \text{ (mód 11)}.$

a) Si x es una solución de $x \equiv 1 \text{ (mód 2)}$, será de la forma $x = 2k+1$. Imponiendo que $x \equiv 1 \text{ (mód 3)}$, llegamos a $2k + 1 \equiv 1 \text{ (mód 3)}$ ó $k \equiv 0 \text{ (mód 3)}$, por lo que $k = 3h$ para algún entero h y $x = 2(3h) + 1 = 6h + 1$, es decir, $x \equiv 1 \text{ (mód 6)}$.

b) Si $x \equiv 3 \pmod 5$, x es de la forma $x = 5k + 3$ para algún entero k. Imponemos que $x \equiv 5 \pmod 7$: $5k + 3 \equiv 5 \pmod 7 \Rightarrow 5k \equiv 2 \pmod 7 \Rightarrow 5k \equiv 30 \pmod 7 \Rightarrow k \equiv 6 \pmod 7 \Rightarrow k = 7h + 6$ para algún entero h. Entonces $x = 35h + 33$ para algún entero h. Ahora sometemos x a la congruencia $x \equiv 7 \pmod{11}$ y obtenemos $35h + 33 \equiv 7 \pmod{11} \Rightarrow 35h \equiv 7 \pmod{11} \Rightarrow\Rightarrow 5h \equiv 1 \pmod{11} \Rightarrow 5h \equiv 45 \pmod{11} \Rightarrow h \equiv 9 \pmod{11}$. Entonces $h = 11m + 9$ para algún entero m, y finalmente $x = 35(11m + 9) + 33 = 385m + 348$ para algún entero m, es decir $x \equiv 348 \pmod{385}$.

c) En primer lugar, $2x \equiv 1 \pmod 5 \Rightarrow 2x \equiv 6 \pmod 5 \Rightarrow x \equiv 3 \pmod 5$, Así que x es de la forma $5k + 3$. Sustituyendo en $3x \equiv 2 \pmod 7$, $15k + 9 \equiv 2 \pmod 7 \Rightarrow k \equiv 0 \pmod 7$. Entonces k es de la forma $7h$ y x es de la forma $35h + 3$, que llevado a la ecuación $4x \equiv 3 \pmod{11}$ la convierte en $140h + 12 \equiv 3 \pmod{11} \Rightarrow 8h \equiv 2 \pmod{11} \Rightarrow 4h \equiv 1 \pmod{11} \Rightarrow h \equiv 3 \pmod{11}$, luego h es de la forma $11m + 3$ y x es de la forma $385h + 108$, es decir $x \equiv 108 \pmod{385}$.

4. **Resolver los sistemas**

a) $x \equiv 1 \pmod 2, x \equiv 2 \pmod 3$

b) $x \equiv 2 \pmod 5, 2x \equiv 3 \pmod 7, 3x \equiv 4 \pmod{11}$

c) $x \equiv 31 \pmod{41}, x \equiv 59 \pmod{26}$

a) Ponemos $x = 2k + 1$ y sustituimos en $x \equiv 2 \pmod 3$, obteniendo $2k + 1 \equiv 2 \pmod 3 \Rightarrow 2k \equiv 1 \pmod 3 \Rightarrow k \equiv 2 \pmod 3 \Rightarrow x = 2(3h + 2) + 1 = 6h + 5 \Rightarrow x \equiv 5 \pmod 6$.

b) x es de la forma $5k + 2$ y como

$$\left.\begin{array}{l} 2x \equiv 3 \pmod 7 \Leftrightarrow x \equiv 5 \pmod 7 \\ 3x \equiv 4 \pmod{11} \Leftrightarrow x \equiv 5 \pmod{11} \end{array}\right\} \Leftrightarrow x \equiv 5 \pmod{77},$$

$5k + 2 \equiv 5 \pmod{77} \Rightarrow 5k \equiv 3 \pmod{77} \Rightarrow k \equiv 16 \pmod{77}$. Entonces, $x = 5(77h + 16) + 2 = 385h + 82$ y, por tanto, $x \equiv 82 \pmod{385}$.

c) Escribiendo $x = 41k + 31$ y sustituyendo en $x \equiv 7$ (mód 26), obtenemos $41k + 31 \equiv 7$ (mód 26) $\Rightarrow 41k \equiv 2$ (mód 26). Usando el algoritmo de Euclides encontramos que $7 \cdot 41 - 11 \cdot 26 = 1$ y por tanto que $14 \cdot 41 - 22 \cdot 26 = 2$, lo que nos permite afirmar que $41k \equiv 2$ (mód 26) $\Leftrightarrow 41k \equiv 2 + 22 \cdot 26 = 574$ (mód 26) $\Leftrightarrow k \equiv 14$ (mód 26). Entonces, $x = 41(26h + 14) + 31 = 1066h + 605 \Rightarrow x = 605$ (mód 1066).

5. **¿Qué posibilidades hay para el número de soluciones de una congruencia lineal módulo 20?**

   Como $20 = 2^2 \cdot 5$, los divisores de 20 son 1, 2, 4, 5, 10 y 20. La congruencia $ax \equiv b$ (mód 20) puede tener, entonces, 1, 2, 4, 5, 10 o 20 soluciones pues ese puede ser el máximo común divisor de a y 20.

6. **Construir congruencias lineales módulo 20 con ninguna solución, con exactamente una solución y con más de una solución. ¿Se puede encontrar una con 20 soluciones?**

   Para encontrar una congruencia que no tenga solución tomamos, por ejemplo $a = 6$, de manera que $(a, 20) = 2$, y ahora elegimos b de manera que $2 \nmid b$, por ejemplo $b = 7$. Entonces la congruencia sería $6x \equiv 7$ (mód 20).

   Para encontrar una congruencia con exactamente una solución, buscamos un a tal que $(a, 20) = 1$ y cualquier b. Por ejemplo, $3x \equiv 1$ (mód 20), cuya única solución es $x = 7$.

   Para encontrar una congruencia con 4 soluciones, elegimos a tal que $(a, 20) = 4$, por ejemplo $a = 8$, y b un múltiplo de 4, por ejemplo $b = 4$. Así obtenemos $8x \equiv 4$ (mód 20), que es equivalente a $2x \equiv 1$ (mód 5) ó $x \equiv 3$ (mód 5), que dan lugar a las soluciones 3, 8, 13 y 18 de la congruencia $8x \equiv 4$ (mód 20).

   Sí hay congruencias módulo 20 que tienen 20 soluciones, por ejemplo $20x \equiv 0$ (mód 20).

7. **Resolver** $9x \equiv 4$ **(mód 1453)**.

   Si x es solución de esta congruencia, existe un entero y tal que $9x - 1453y = 4$. Usando el algoritmo de Euclides encontramos que $9 \cdot 339 - 1453 \cdot 2 = 1$, y por tanto que $9 \cdot 1292 - 1453 \cdot 8 = 4$. Entonces $9x \equiv 4$ (mód 1453) $\Leftrightarrow x \equiv 1292$ (mód 1453).

8. **Resolver $4x \equiv 9$ (mód 1453).**

   Si x es solución de esta congruencia, existe un entero y tal que $4x - 1453y = 9$. Con el algoritmo de Euclides encontramos que $4 \cdot (-363) + 1453 \cdot 1 = 1$, y por tanto que $4 \cdot (-3267) + 1453 \cdot 9 = 9$. Entonces la congruencia propuesta es equivalente a $x \equiv -3267 \equiv 3 \cdot 1453 - 3267 = 1092$ (mód 1453).

9. Resolver en x e y:

   a) $x + 2y \equiv 3$ **(mód 7)**, $3x + y \equiv 2$ **(mód 7)**.

   b) $x + 2y \equiv 3$ **(mód 6)**, $3x + y \equiv 2$ **(mód 6)**.

   a) Usamos el método de sustitución, reduciendo módulo 7:
   $x = 3 - 2y \Rightarrow 9 - 6y + y = 2 \Rightarrow 5y = 0 \Rightarrow y = 0 \Rightarrow x = 3$.

   b) Ahora módulo 6: $y = 2 - 3x \Rightarrow x + 4 - 6x = 3 \Rightarrow 5x = 1 \Rightarrow x = 5 \Rightarrow y = 2 - 15 = -13 = 5$.

10. **Resolver en x e y:**

    a) $x + 2y \equiv 3$ (mód 9), $3x + y \equiv 2$ (mód 9).

    b) $x + 2y \equiv 3$ (mód 10), $3x + y \equiv 2$ (mód 10).

    a) Usamos el método de sustitución, reduciendo módulo 9:
    $x = 3 - 2y \Rightarrow 9 - 6y + y = 2 \Rightarrow -5y = 2 \Rightarrow 4y = 2 \Rightarrow 2y = 1 \Rightarrow y = 5 \Rightarrow x = -7 = 2$.

    b) Ahora módulo 10: $y = 2 - 3x \Rightarrow x + 4 - 6x = 3 \Rightarrow 5x = 1$. En este caso, la congruencia no tiene solución, pues $(a, m) = (5, 10) = 5$ no divide a $b = 1$.

11. **Cuando los participantes en el Desfile del Departamento de Matemáticas se alinearon de 4 en 4, sobraba una persona; cuando lo intentaron de 5 en 5, sobraban dos personas y cuando iban de 7 en 7, sobraban 3. ¿Cómo de grande es el Departamento?**

    Se trata de resolver el sistema

$$x \equiv 1 \text{ (mód 4)}, \quad x \equiv 2 \text{ (mód 5)}, \quad x \equiv 3 \text{ (mód 7)},$$

Si $x = 4k + 1$, entonces $4k + 1 \equiv 2$ (mód 5) $\Rightarrow 4k \equiv 1$ (mód 5) $\Rightarrow k \equiv 4$ (mód 5) $\Rightarrow k = 5h + 4 \Rightarrow x = 20h + 17 \Rightarrow 20h + 17 \equiv 3$ (mód 7) $\Rightarrow 6h \equiv 0$ (mód 7) $\Rightarrow h \equiv 0$ (mód 7) $\Rightarrow h = 7m \Rightarrow x = 140m + 17$.

El número de miembros del Departamento puede ser 17, 157, etc.

12. **Encontrar un múltiplo de 7 que deje resto 1 cuando se divide por 2, 3, 4, 5 o 6**.

    Si N da resto 1 al dividir por 2, 3, 4, 5 o 6, $N - 1$ es un múltiplo de $2 \cdot 3 \cdot 4 \cdot 5 \cdot 6 = 720$. Entonces buscamos una solución de la ecuación $7n - 1 = 720k$. Usando el algoritmo de Euclides encontramos que $7 \cdot 103 - 720 \cdot 1 = 1$, por lo que $n = 103$ nos da la solución $N = 721$.

13. **Encontrar el menor impar n, $n > 3$ tal que $3|n$, $5|n+2$ y $7|n+4$.**

    Buscamos un $n > 3$ tal que $2|n-3$, $3|n-3$, $5|n-3$ y $7|n-3$, por tanto $n - 3$ es un múltiplo de $2 \cdot 3 \cdot 5 \cdot 7 = 210$. El menor número $n > 3$ es $210 + 3 = 213$.

14. **Encontrar el menor entero n, $n > 2$ tal que $2|n$, $3|n+1$, $4|n+2$, $5|n+3$ y $6|n+4$.**

    Buscamos un $n > 2$ tal que $2|n-2$, $3|n-2$, $4|n-2$, $5|n-2$ y $6|n-2$. Por tanto, 60 divide a $n - 2$. El menor valor posible de n es, entonces, $n = 60 + 2 = 62$.

15. **Encontrar un entero positivo tal que su mitad es un cuadrado, su tercera parte es un cubo y su quinta parte es una quinta potencia**.

    Escribimos el número en la forma $N = 2^a 3^b 5^c$, con lo que $\frac{N}{2} = 2^{a-1} 3^b 5^c$, $\frac{N}{3} = 2^a 3^{b-1} 5^c$ y $\frac{N}{5} = 2^a 3^b 5^{c-1}$.

    Como $\frac{N}{2}$ es un cuadrado y $\frac{N}{3}$ es un cubo, c debe ser un múltiplo de 6, y como $\frac{N}{5}$ es una quinta potencia, $c - 1$ debe ser múltiplo de 5. $c = 6$ cumple estas dos condiciones.

    Análogamente, Como $\frac{N}{2}$ es un cuadrado y $\frac{N}{5}$ es una quinta potencia, b debe ser un múltiplo de 10, y como $\frac{N}{3}$ es un cubo, $c - 1$ debe ser múltiplo de 3. $b = 10$ cumple estas dos condiciones.

    Análogamente, Como $\frac{N}{3}$ es un cubo y $\frac{N}{5}$ es una quinta potencia, a debe ser un múltiplo de 15, y como $\frac{N}{2}$ es un cuadrado, $a - 1$ debe ser par. $a = 15$ cumple estas dos condiciones.

Por tanto, una solución es $N = 2^{15}3^{10}5^6 = 30,233,088,000,000$.

16. **Cada uno de los números consecutivos 48, 49 y 50 tiene un factor cuadrado**.

   a) **Encontrar** n **tal que** $3^2|n$**,** $4^2|n+1$ **y** $5^2|n+2$.

   b) **¿Puede encontrarse un** n **tal que** $2^2|n$**,** $3^2|n+1$ **y** $4^2|n+2$**?**.

   a) Buscamos un n tal que $9|n$, $16|n+1$ y $25|n+2$, o lo que es lo mismo, una solución del sistema

   $$n \equiv 0 \text{ (mód 9)}, \quad n \equiv -1 \text{ (mód 16)}, \quad n \equiv -2 \text{ (mód 25)}.$$

   Escribiendo $n = 9k \equiv -1$ (mód 16), llegamos a $9k \equiv 63$ (mód 16) ó $k \equiv 7$ (mód 16). Entonces $k = 16h + 7$ y $n = 144h + 63$ para algún h.

   Ahora $144h + 63 \equiv -2$ (mód 25) $\Rightarrow 19h \equiv 10$ (mód 25)

   b) Si $4|n$ y $16|n+2$, sería $n \equiv 0$ (mód 4), $n \equiv -2$ (mód 16), y entonces para algún k tendríamos $4k \equiv -2$ (mód 16), que es imposible, pues $(4, -16) = 4$ no divide a -2.

17. **Si** $x \equiv r$ (mód m) **y** $x \equiv s$ (mód $m+1$), **demostrar que**

$$x \equiv r(m+1) - sm \text{ (mód } m(m+1)).$$

Expresemos $x = km + r$ y $x = h(m+1) + s$. Entonces

$$\begin{aligned} r(m+1) - sm = & \quad (x - km)(m+1) - (x - h(m+1))m = \\ = & \quad (m+1)x - km(m+1) - mx + hm(m+1) = \\ = & \quad x + (h-k)m(m+1). \end{aligned}$$

18. **¿Qué enteros positivos, después de ser multiplicados por 3, 5 y 7 respectivamente y los productos divididos por 20, dan restos en progresión aritmética con diferencia común 1 y cocientes iguales a los restos?**

Llamando a, b, c a los tres números, el problema queda planteado así:

$$\begin{cases} 3a = 20q + q \\ 5b = 20(q+1) + (q+1) \\ 7c = 20(q+2) + (q+2) \end{cases} \Rightarrow \begin{cases} 3a = 21q \\ 5b = 21(q+1) \\ 7c = 21(q+2) \end{cases} \Rightarrow \begin{cases} 5b - 3a = 21 \\ 7c - 3a = 42 \end{cases}.$$

Resolviendo la primera de las ecuaciones obtenemos

$$\begin{cases} a = 53 + 5t \\ b = 42 + 3t \end{cases},$$

Siendo a múltiplo de 7, también debe serlo t, pongamos $t = 7s$, y entonces $a = 63 + 35s = 7(9 + 5s)$, es decir $q = 9 + 5s$.

Para $s = 0$, obtenemos $q = 9$ y

$$\begin{array}{ll} a = 63, & 3a = 189 = 20 \cdot 9 + 9 \\ b = 42, & 5b = 210 = 20 \cdot 10 + 10 \\ c = 33, & 7c = 231 = 20 \cdot 11 + 11 \end{array}$$

Para $s = 1$, obtenemos $q = 14$ y

$$\begin{array}{ll} a = 98, & 3a = 294 = 20 \cdot 14 + 14 \\ b = 63, & 5b = 315 = 20 \cdot 15 + 15 \\ c = 48, & 7c = 336 = 20 \cdot 16 + 16. \end{array}$$

19. **Supongamos que los módulos del sistema**

$$x = a_i \ (\text{mód } m_i) \quad i = 1, 2, \cdots, k$$

no son primos relativos dos a a dos. Encontrar una condición que deban cumplir los a_i para que el sistema tenga solución.

La condición $(m_i, m_j)|(a_i - a_j)$ para todo i, j es necesaria y suficiente para que el sistema tenga solución.

En efecto, supongamos que el sistema tiene solución. Entonces existe un x_0 tal que $m_i|(x_0 - x_i) \quad i = 1, 2, \cdots, k$. Si $1 \leq i, j \leq k$, como (m_i, m_j) es un divisor de m_i y de m_j, también lo será de $x_0 - x_i$ y de $x_0 - x_j$ y, por tanto, de su diferencia $x_i - x_j$.

Para demostrar el recíproco, vamos a tener en cuenta que cada congruencia $x = a$ (mód m) puede descomponerse en un sistema de congruencias primarias $x = a$ (mód $p_i^{e_i}$) (llamadas así porque sus módulos son potencias de primos) , siendo $p_1^{e_1} \cdots p_r^{e_r}$ la descomposición canónica de m en factores primos.

Supongamos, entonces, que se cumple que $(m_i, m_j)|(a_i - a_j)$ para todo i, j. Si se cumple que $(m_i, m_j) = 1$ para todos los $i \neq j$, entonces

sabemos que el sistema tiene solución por el teorema chino del resto. Si no es así, una vez que descomponemos cada congruencia del sistema en un sistema de congruencias primarias, nos encontraremos con pares de congruencias del tipo

$$\begin{cases} x = a_i \ (\text{mód } p^s) \\ x = a_j \ (\text{mód } p^t) \end{cases},$$

En este sistema de congruencias, si $s \leq t$, p^s es un divisor de p^t y si x es una solución de la segunda congruencia, también lo va a ser de la primera pues $p^t|(x - a_j) \Rightarrow p^s|(x - a_j) \Rightarrow p^s|(x - a_i)$, cumpliéndose la última implicación por la hipótesis $(m_i, m_j)|(a_i - a_j)$. Esto nos dice que son superfluas las congruencias cuyos módulos sean potencias inferiores, por lo que pueden eliminarse. Al final, nos va a quedar un sistema de congruencias primarias en las formadas por las potencias con mayor exponente, que son las que se usan para construir el mínimo común múltiplo. Estas potencias de mayor exponente no tienen factores comunes, por lo que el teorema chino del resto nos garantiza una solución del sistema.

Por ejemplo, resolvamos el sistema de congruencias

$$\begin{cases} x \equiv 5 \ (\text{mód } 6) \\ x \equiv 2 \ (\text{mód } 15) \\ x \equiv 7 \ (\text{mód } 20) \end{cases}$$

En ese caso, $(6, 15) = 3$ divide a $5 - 2$, $(6, 20) = 2$ divide a $5 - 7$, y $(15, 20) = 5$ divide a $2 - 7 = 5$, por lo que el sistema tiene solución. Ahora, transformamos el sistema en uno de congruencias primarias:

$$\begin{cases} x \equiv 5 \ (\text{mód } 2) \\ x \equiv 5 \ (\text{mód } 3) \\ x \equiv 2 \ (\text{mód } 3) \\ x \equiv 2 \ (\text{mód } 5) \\ x \equiv 7 \ (\text{mód } 4) \\ x \equiv 7 \ (\text{mód } 5) \end{cases}$$

La primera es superflua porque el módulo de la penúltima tiene mayor exponente. La segunda es equivalente a la tercera. La última es equivalente a la cuarta. Por tanto, eliminando las congruencias superfluas

nos queda:

$$\begin{cases} x \equiv 2 \text{ (mód 3)} \\ x \equiv 2 \text{ (mód 5)} \\ x \equiv 7 \text{ (mód 4)} \end{cases} \Rightarrow \begin{cases} x \equiv 2 \text{ (mód 3)} \\ x \equiv 2 \text{ (mód 5)} \\ x \equiv 3 \text{ (mód 4)} \end{cases}$$

Para resolver esta congruencia el método usado en la demostración del teorema chino del resto en varios textos, por ejemplo en el de Niven y Zuckermann.

El producto de los módulos $m_1 = 3$, $m_2 = 5$ y $m_3 = 4$ es $M = 60$. Dividiendo M por 3, 5 y 4 obtenemos $M_1 = 20$, $M_2 = 12$ y $M_3 = 15$, respectivamente.

Ahora hallamos números x_i, y_i tales que $M_i x_i + m_i y_i = 1$, $(1 \leq i \leq 3)$:

$$\begin{array}{lll} 20 \cdot (-1) + 3 \cdot 7 = 1, & x_1 = -1, & y_1 = 7 \\ 12 \cdot (-2) + 5 \cdot 5 = 1, & x_2 = -2, & y_2 = 5 \\ 15 \cdot (-1) + 4 \cdot 4 = 1, & x_3 = -1, & y_3 = 4 \end{array}$$

Una solución del sistema viene dada por:

$$\begin{aligned} x =& 2 \cdot M_1 \cdot x_1 + 2 \cdot M_2 \cdot x_2 + 3 \cdot M_3 \cdot x_3 = \\ =& 2 \cdot 20 \cdot (-1) + 2 \cdot 12 \cdot (-2) + 3 \cdot 15 \cdot (-1) = \\ =& -133 = -13 \text{ (mód 60)} = 47 \text{ (mód 60)}. \end{aligned}$$

20. **¿Cuántos múltiplos de b hay en la sucesión $a, 2a, 3a, \cdots, ba$?**

xa es un múltiplo de b si y solo si x es una solución $ax \equiv 0$ (mód b), y el número de soluciones de esta congruencia es (a, b), es decir el máximo común divisor de a y b.

6. Los teoremas de Fermat y Wilson

1. **¿Cuál es el resto de 5^6 (mód 7), 5^8 (mód 7) y 1945^8 (mód 7)?**

   Por el teorema de Fermat, $5^6 \equiv 1$ (mód 7). Como consecuencia, $5^8 \equiv 5^2 \equiv 4$ (mód 7). Ahora usamos que $1945 \equiv 6$ (mód 7) y que $6^6 \equiv 1$ (mód 7). Entonces: $1945^8 \equiv 6^8 \equiv 6^2 \equiv 1$ (mód 7).

2. **¿Cuál es el resto de 5^{10} (mód 11), 5^{12} (mód 11) y de 1945^{12} (mód 11)?**

   Por el teorema de Fermat, $5^{10} \equiv 1$ (mód 11). Como consecuencia, $5^{12} \equiv 5^2 \equiv 3$ (mód 11). Ahora usamos que $1945 \equiv 9$ (mód 11) y que $9^{10} \equiv 1$ (mód 11). Entonces: $1945^{12} \equiv 9^{12} \equiv 9^2 \equiv 4$ (mód 11).

3. **¿Cuál es el último dígito de 7^{355}?**

   Hallamos las primeras potencias de 7 y obtenemos: $7^2 \equiv 9$ (mód 10), $7^3 \equiv 3$ (mód 10), $7^4 \equiv 1$ (mód 10). Como $355 = 4 \cdot 88 + 3$, $7^{355} \equiv 7^3 \equiv 3$ (mód 10) y 7^{355} acaba en 3.

4. **¿Cuáles son los dos últimos dígitos de 7^{355}?**

   Las primeras potencias de 7 son $7, 49, 343, 2401$.

   Entonces $7^4 \equiv 1$ (mód 100) y como $355 = 4 \cdot 88 + 3$, $7^{355} \equiv 7^3 \equiv 43$ (mód 100) y 7^{355} acaba en 43.

5. **¿Cuál es el resto de dividir 314^{162} por 163?**

   Basta tomar $a = 314$ y $p = 163$ y obtenemos, por el teorema de Fermat, $314^{162} \equiv 1$ (mód 163).

6. **¿Cuál es el resto de dividir 314^{162} por 7?**

   Tomando, $a = 314$ y $p = 7$ y obtenemos, por el teorema de Fermat, $314^6 \equiv 1$ (mód 7). Entonces $314^{162} = (314^6)^{27} \equiv 1$ (mód 7) $= 1$ (mód 7).

7. **¿Cuál es el resto de dividir 314^{164} por 165? (¡Observar que 165 no es primo!)**

   Descomponemos $165 = 3 \cdot 5 \cdot 11$ y $314 = 2 \cdot 157$. Por el teorema de Fermat, $314^2 \equiv 1$ (mód 3), $314^4 \equiv 1$ (mód 5) y $314^{10} \equiv 1$ (mód 11).

Por tanto:

$$\begin{array}{l} 314^{164} = 314^{2\cdot 82} \equiv 1 \text{ (mód 3)} \\ 314^{164} = 314^{4\cdot 41} \equiv 1 \text{ (mód 5)} \\ 314^{164} = 314^{10\cdot 31+4} \equiv 314^4 \equiv 6^4 \equiv 3^2 = 9 \text{ (mód 11)} \end{array},$$

Entonces de donde deducimos que 314^{164} es una solución del sistema:

$$\begin{cases} x \equiv 1 \text{ (mód 15)} \\ x \equiv 9 \text{ (mód 11)} \end{cases}$$

El producto de los módulos $m_1 = 11$ y $m_2 = 15$ es $M = 165$. Dividiendo M por 15 y 11 obtenemos $M_1 = 11$ y $M_2 = 15$, respectivamente.

Ahora hallamos números x_i, y_i tales que $M_i x_i + m_i y_i = 1$, $(1 \leq i \leq 2)$:

$$\begin{array}{lll} 11 \cdot (-4) + 15 \cdot 3 = 1, & x_1 = -4, & y_1 = 3 \\ 15 \cdot 3 + 11 \cdot (-4) = 1, & x_2 = 3, & y_2 = -4 \end{array}$$

La solución del sistema viene dada por:

$$\begin{aligned} x =& 1 \cdot M_1 \cdot x_1 + 9 \cdot M_2 \cdot x_2 = \\ =& 1 \cdot 11 \cdot (-4) + 9 \cdot 15 \cdot 3 = \\ =& 361 \equiv 31 \text{ (mód 165)}. \end{aligned}$$

8. **¿Cuál es el resto de dividir 2001^{2001} por 26?**

Como $26 = 2 \cdot 13$, Hallemos los restos de dividir 2001^{2001} por 2 y por 13. Evidentemente, $2001^{2001} \equiv 1$ (mód 2). Por el teorema de Fermat, $2001^{12} \equiv 1$ (mód 13). Usando que, $2001 = 166 \cdot 12 + 9$, y que $2001 \equiv -1$ (mód 13), $2001^{2001} \equiv 2001^9 \equiv (-1)^9 = -1$ (mód 13). Por tanto 2001^{2001} será congruente, módulo 26 con la solución del sistema

$$\begin{cases} x \equiv 1 \text{ (mód 2)} \\ x \equiv -1 \text{ (mód 13)} \end{cases}$$

El producto de los módulos es $M = 26$. Dividiendo M por 2 y 13 obtenemos $M_1 = 13$ y $M_2 = 2$, respectivamente.

Ahora hallamos números x_i, y_i tales que $M_i x_i + m_i y_i = 1$, $(1 \leq i \leq 2)$:

$$\begin{array}{lll} 13 \cdot 1 + 2 \cdot (-6) = 1, & x_1 = 1, & y_1 = -6 \\ 2 \cdot (-6) + 13 \cdot 1 = 1, & x_2 = -6, & y_2 = 1 \end{array}$$

Una solución del sistema viene dada por:

$$\begin{aligned} x =& 1 \cdot M_1 \cdot x_1 + (-1) \cdot M_2 \cdot x_2 = \\ =& 1 \cdot 13 \cdot 1 + (-1) \cdot 2 \cdot (-6) = \\ =& 25 \text{ (mód 26)}. \end{aligned}$$

9. **Demostrar que**

$$(p-1)(p-2)\cdots(p-r) \equiv (-1)^r r! \ \textbf{(mód } p),$$

para $r = 1, 2, \ldots, p-1$.

$$\begin{aligned} (p-1)(p-2)\cdots(p-r) &\equiv (-1)(-2)\cdots(-r) = \\ &= \underbrace{(-1)\cdots(-1)}_{r \text{ veces}} \cdot 1 \cdot 2 \cdots r = \\ &= (-1)^r r! \text{ (mód } p) \end{aligned}$$

10. *a*) **Calcular** $(n-1)!$ (mód n) **para** $n = 10, 12, 14$ **y** 15.

$$\begin{aligned} &(10-1)! = 9 \cdot 8 \cdot 7 \cdot 6 \cdot \boxed{5} \cdot 4 \cdot 3 \cdot \boxed{2} \cdot 1 = 0 \text{ (mód } 10) \\ &(12-1)! = 11 \cdot 10 \cdot 9 \cdot 8 \cdot 7 \cdot \boxed{6} \cdot 5 \cdot 4 \cdot 3 \cdot \boxed{2} \cdot 1 = 0 \text{ (mód } 12) \\ &(14-1)! = 13 \cdots 8 \cdot \boxed{7} \cdot 6 \cdot 5 \cdot 4 \cdot 3 \cdot \boxed{2} \cdot 1 = 0 \text{ (mód } 14) \\ &(15-1)! = 14 \cdots 7 \cdot 6 \cdot \boxed{5} \cdot 4 \cdot \boxed{3} \cdot 2 \cdot 1 = 0 \text{ (mód } 15) \end{aligned}$$

b) **Enunciar un teorema y demostrarlo**.

Si p es primo sabemos que $(p-1)! \equiv -1$ (mód p), según el teorema de Wilson. El apartado anterior muestra que si n es cualquiera de los números 10, 12, 14 y 15, entonces $(n-1)! \equiv 0$ (mód n). Podemos pensar que esto va a ser cierto cuando n no sea primo.

En efecto, si no es primo podrá descomponerse en la forma $n = ab$ y tanto a como b son distintos de 1 y de n, ambos son números menores que n. Si a y b pueden elegirse distintos, ambos aparecerán en el desarrollo de $(n-1)!$, por lo que $(n-1)! \equiv 0$ (mód n). El único caso en el que no pueden elegirse a y b distintos es aquél en que $n = p^2$, siendo p un primo. Exceptuando a su vez el caso $p = 2$ (ó $n = 4$), que puede comprobarse directamente ($(4-1)! = 6$

no es divisible por 4), p y $2p$ serán siempre dos números menores que p^2-1. Por ello, p y $2p$ aparecerán en el desarrollo de $(n-1)! = (p^2-1)!$ y si $n = p^2$, será $(n-1)! \equiv 0$ (mód n). La conclusión es: *Si $n > 4$ no es primo, entonces $(n-1)! \equiv 0$ (mód n).*

11. **Demostrar que** $2(p-3)! + 1 \equiv 0$ (mód p).

    (Suponemos que p es un primo impar mayor o igual que 3). Usando que

$$\begin{aligned}(p-1)! =&(p-1)(p-2)(p-3)! = \\ =&(p^2-3p+2)(p-3)! \equiv \\ \equiv&2(p-3)! \text{ (mód } p)\end{aligned}$$

    y el teorema de Wilson, obtenemos que $-1 \equiv 2(p-3)!$ (mód p), que es lo que queríamos demostrar.

12. **En 1732 Euler escribió: "He obtenido resultados [correctos] a partir de un teorema elegante, de cuya veracidad estoy seguro, aunque no tengo demostración: $a^n - b^n$ es divisible por el primo $n+1$ si ni a y b lo son". Demostrar este teorema, usando el teorema de Fermat**.

    Basta tener en cuenta que si $n+1$ no divide ni a a ni a b, entonces, por el teorema de Fermat, tendremos que $a^n \equiv 1$ (mód $(n+1)$) y $b^n \equiv 1$ (mód $(n+1)$), de donde $a^n - b^n \equiv 0$ (mód $(n+1)$) es divisible por $n+1$.

13. **Observar que**

$$\begin{array}{lrl} 6! & \equiv & -1 \quad (\text{mód } 7) \\ 5!1! & \equiv & 1 \quad (\text{mód } 7) \\ 4!2! & \equiv & -1 \quad (\text{mód } 7) \\ 3!3! & \equiv & 1 \quad (\text{mód } 7) \end{array}$$

    Hacer el mismo tipo de cálculos (mód 11).

    La instrucción de *Mathematica*,

```
Table[{(10-t)!t!, Mod[(10-t)!t!,11]},{t,0,5}]
```

nos permite afirmar que

$$\begin{array}{rrcrl} 10! = & 3628800 & \equiv & -1 & (\text{mód } 11) \\ 9!1! = & 362880 & \equiv & 1 & (\text{mód } 11) \\ 8!2! = & 80640 & \equiv & -1 & (\text{mód } 11) \\ 7!3! = & 30240 & \equiv & 1 & (\text{mód } 11) \\ 6!4! = & 17280 & \equiv & -1 & (\text{mód } 11) \\ 5!5! = & 14400 & \equiv & 1 & (\text{mód } 11) \end{array}$$

14. **Enunciar un teorema a partir de los datos del problema 13, y demostrarlo**.

El teorema puede enunciarse así: Si p es primo y $0 \leq r < p$, entonces $(p-1-r)!r! = (-1)^{r+1}$ (mód p). Si usamos (ejercicio 9) que $(p-1)(p-2)\cdots(p-r) \equiv (-1)^r r!$ (mód p), obtenemos:

$$\begin{array}{rcl} (p-1)! & = & (p-1)(p-2)\cdots(p-r)\ (p-1-r)\ ! \\ -1 & \equiv & (-1)^r r!(p-1-r)! \ (\text{mód } p) \\ r!(p-1-r)! & \equiv & (-1)^{r+1} \ (\text{mód } p) \end{array}$$

15. **Supongamos que p es un primo impar**.

a) **Demostrar que** $1^{p-1} + 2^{p-1} + \cdots + (p-1)^{p-1} \equiv -1$ (mód p).

b) **Demostrar que** $1^p + 2^p + \cdots + (p-1)^p \equiv 0$ (mód p).

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

b) $1^p + 2^p + \cdots + (p-1)^p \equiv 1 + 2 + \cdots + p = \frac{p-1}{2}p \equiv 0$ (mód p).

16. **Demostrar que el recíproco del teorema de Fermat es falso. [Superpista: Considerar 2^{340} (mód 341)]**.

$341 = 11 \cdot 31$ no es primo. Hallemos 2^{340} (mód 11) y 2^{340} (mód 31). Según el teorema de Fermat, $2^{10} = 1$ (mód 11), por lo que $2^{340} = (2^{10})^{34} \equiv 1$ (mód 11). De la misma forma, como $2^5 \equiv 1$ (mód 31), $2^{340} = 2^{68 \cdot 5} \equiv 1$ (mód 31). Entonces, obtenemos $2^{340} \equiv 1$ (mód 341). Vemos entonces que la relación $a^{n-1} \equiv 1$ (mód n) no implica que n sea primo.

17. **Demostrar que para cualesquiera dos primos diferentes p y q,**

a) $pq|(a^{p+q} - a^{p+1} - a^{q+1} + a^2)$

b) $pq|(a^{pq} - a^p - a^q + a)$

a) Usamos el teorema de Fermat y obtenemos que $a^p \equiv a \pmod{p}$ y que $a^q \equiv a \pmod{q}$, $p|(a^p - a)$ y $q|(a^q - a)$, de donde pq divide a $(a^p - a)(a^q - a) = (a^{p+q} - a^{p+1} - a^{q+1} + a^2)$.

b) Demostremos que q divide a $a^{pq} - a^p - a^q + a$. Usando el teorema de Fermat, obtenemos que $a^{p-1} \equiv 1 \pmod{p}$ y que $a^{q-1} \equiv 1 \pmod{q}$. Elevando a p, $a^{p(q-1)} \equiv 1 \pmod{q}$ y de ahí, $a^{pq} - a^p - a^q + a^2 = a^p(a^{pq-p} - 1) + a(1 - a^{q-1})$ es divisible por q.

De forma parecida se demuestra que p divide a $a^{pq} - a^p - a^q + a$.

18. **Demostrar que si p es un primo impar, entonces $2p|(2^{2p-1} - 2)$.**

Usando el teorema de Fermat, $2^{p-1} \equiv 1 \pmod{p}$ y, elevando al cuadrado, $2^{2p-2} \equiv 1 \pmod{p}$, es decir, $2^{2p-2} = 1 + kp$ para un cierto entero k. Multiplicando esta igualdad por 2, obtenemos $2^{2p-1} = 2 + k(2p)$, es decir, $2^{2p-1} - 2$ es un múltiplo de $2p$.

19. **¿Para qué enteros n es cierto que $p|(1 + n + n^2 + \cdots + n^{p-2})$?**

Si $p|n$, entonces no es cierta la relación, pues $p|n$ y $p|(1 + n + n^2 + \cdots + n^{p-2})$ implica que $p|1$.

Si $p|(n-1)$, entonces tampoco es cierta la relación, pues tenemos $n \equiv 1 \pmod{p}$ y $p|(1 + n + n^2 + \cdots + n^{p-2}) \equiv -1 \pmod{p}$.

Si $p \nmid n$ y $p \nmid (n-1)$ sí es cierta la relación pues

$$1 + n + n^2 + \cdots + n^{p-2} = \frac{n^{p-1} - 1}{n - 1} \equiv \frac{0}{n-1} = 0 \pmod{p}$$

20. **Demostrar que todo primo impar n excepto el 5 divide a algún número de la forma $111\cdots11$ (k dígitos, todos unos).**

Si p es un primo impar distinto de 5, p no divide a 10. El único p que divide a $10 - 1 = 9$ es $p = 3$ que divide a 111. Para los demás p, el ejercicio anterior nos dice que p es un divisor de

$$\underbrace{111\cdots11}_{p-1 \text{ unos}} = 1 + 10 + 10^2 + \cdots + 10^{p-2}.$$

7. Los divisores de un entero

1. **Calcular** $d(42)$**,** $\sigma(42)$**,** $d(420)$ **y** $\sigma(42)$.

   Si $n = p_1^{e_1} \cdot p_2^{e_2} \cdots p_r^{e_r}$, entonces:

   $$d(n) = (e_1 + 1) \cdot (e_2 + 1) \cdots (e_r + 1)$$
   $$\sigma(n) = \frac{p_1^{e_1+1} - 1}{p_1 - 1} \cdot \frac{p_2^{e_2+1} - 1}{p_2 - 1} \cdots \frac{p_r^{e_r+1} - 1}{p_r - 1}$$

   Como $42 = 2^1 \cdot 3^1 \cdot 7^1$,

   $$d(42) = 2 \cdot 2 \cdot 2 = 8, \quad \sigma(42) = \frac{2^2 - 1}{2 - 1} \cdot \frac{3^2 - 1}{3 - 1} \cdot \frac{7^2 - 1}{7 - 1} = 3 \cdot 4 \cdot 8 = 96.$$

   Como $420 = 2^2 \cdot 3^1 \cdot 5^1 \cdot 7^1$,

   $$d(420) = 3 \cdot 2 \cdot 2 \cdot 2 = 24,$$
   $$\sigma(420) = \frac{2^3 - 1}{2 - 1} \cdot \frac{3^2 - 1}{3 - 1} \cdot \frac{5^2 - 1}{5 - 1} \cdot \frac{7^2 - 1}{7 - 1} = 7 \cdot 4 \cdot 6 \cdot 8 = 1344.$$

2. **Calcular** $d(540)$, $\sigma(540)$, $d(5400)$, **y** $\sigma(5400)$.

   Como $540 = 2^2 \cdot 3^3 \cdot 5^1$,

   $$d(540) = 3 \cdot 4 \cdot 2 = 24,$$
   $$\sigma(540) = \frac{2^3 - 1}{2 - 1} \cdot \frac{3^4 - 1}{3 - 1} \cdot \frac{5^2 - 1}{5 - 1} = 7 \cdot 40 \cdot 6 = 1680.$$

   Como $540 = 2^3 \cdot 3^3 \cdot 5^2$,

   $$d(540) = 4 \cdot 4 \cdot 3 = 48,$$
   $$\sigma(540) = \frac{2^4 - 1}{2 - 1} \cdot \frac{3^4 - 1}{3 - 1} \cdot \frac{5^3 - 1}{5 - 1} = 15 \cdot 40 \cdot 31 = 18600.$$

3. **Calcular** d **y** σ **para** $10115 = 5 \cdot 7 \cdot 17^2$ **y** $100115 = 5 \cdot 20023$.

   $$d(10115) = 2 \cdot 2 \cdot 3 = 12,$$
   $$\sigma(10115) = (1 + 5) \cdot (1 + 7) \cdot \frac{17^3 - 1}{17 - 1} = 6 \cdot 8 \cdot 307 = 14736.$$

   $$d(100115) = 2 \cdot 2 = 4,$$
   $$\sigma(100115) = (1 + 5)(1 + 20023) = 6 \cdot 20024 = 120144.$$

4. **Calcular d y σ para $10116 = 2^2 \cdot 3^2 \cdot 281$ y $100116 = 2^2 \cdot 3^5 \cdot 103$.**

   Para 10116:

   $$d = 3 \cdot 3 \cdot 2 = 18,$$
   $$\sigma = (1 + 2 + 4) \cdot (1 + 3 + 9) \cdot (1 + 281) = 7 \cdot 13 \cdot 282 = 25662.$$

   Para 100116:

   $$d = 3 \cdot 6 \cdot 2 = 36,$$
   $$\sigma = (1 + 2 + 4) \cdot \frac{3^6 - 1}{3 - 1} \cdot (1 + 103) = 7 \cdot 364 \cdot 104 = 264992.$$

5. **Demostrar que $\sigma(n)$ es impar si n es una potencia de 2.**

   Si $n = 2^r$, entonces $\sigma(n) = 1 + 2 + \cdots + 2^r = \frac{2^{r+1}-1}{2-1} = 2^{r+1} - 1$, que es un número impar.

6. **Demostrar que si $f(n)$ es multiplicativa, también lo es $f(n)/n$.**

   Sea $f(n)$ multiplicativa y sea $g(n) = f(n)/n$. Entonces, si m y n son enteros positivos tales que $(m, n) = 1$, se cumplirá que

   $$g(mn) = \frac{f(mn)}{mn} = \frac{f(m)f(n)}{mn} = \frac{f(m)}{m} \cdot \frac{f(n)}{n} = g(m)g(n),$$

   es decir, g es también una función multiplicativa.

7. **¿Cuál es el menor entero n tal que $d(n) = 8$? ¿Y el menor tal que $d(n) = 10$?**

   Si $n = p_1^{e_1} \cdot p_2^{e_2} \cdots p_r^{e_r}$, entonces: $d(n) = (e_1 + 1) \cdot (e_2 + 1) \cdots (e_r + 1)$.

   8 se descompone propiamente de dos formas $2 \cdot 4$ y $2 \cdot 2 \cdot 2$, es decir que un número con 8 divisores será de la forma $n = pq^3$ ó $n = pqr$. En el primer caso, para $p = 3, q = 2$, obtenemos $n = 24$, y en el segundo, para $p = 2, q = 3, r = 5$, obtenemos $n = 30$. Por tanto, el n más pequeño con $d(n) = 8$ es $n = 24$.

   10 se descompone sólo de una forma $2 \cdot 5$. Un número con diez divisores será de la forma $n = p \cdot q^4$. El más pequeño de todos ellos se obtiene para $p = 3, q = 2$ y es $n = 48$.

8. **¿Tiene $d(n) = k$ una solución n para cualquier k?**

   Sí. Dado el número k, el número p^{k-1} tiene k divisores, por lo que $d(n) = k$.

9. **En 1644, Mersenne preguntaba por un número con 60 divisores. Encontrar uno menor que 10,000**.

   De cualquier descomposición de 60 podremos obtener números con 60 divisores. Por ejemplo, de la descomposición trivial $60 = 60$, obtendremos que p^{59}, con p primo tiene 60 divisores, pero $2^{59} > 10000$ y no nos sirve. Puede servir el número $n = 2^4 \cdot 3^2 \cdot 5 \cdot 7 = 5040$, que tiene $5 \cdot 3 \cdot 2 \cdot 2 = 60$ divisores.

10. **Encontrar infinitos números n tales que $d(n) = 60$.**

    Cualquier número de la forma p^{59}, siendo p primo, tiene 60 divisores.

11. **Si p es un primo impar, ¿para qué valores de k es impar la expresión $1 + p + \cdots + p^k$?**

    Si p es impar, también lo es cualquier potencia de p, por lo que la suma $1 + p + \cdots + p^k$, de $k + 1$ números impares, será impar cuando k sea par.

12. **¿Para qué números n es impar $\sigma(n)$?**

    Si $n = p_1^{e_1} \cdots p_r^{e_r}$, $\sigma(n) = (1 + \cdots + p_1^{e_1}) \cdots (1 + \cdots + p_r^{e_r})$ será impar si y solo todos los paréntesis son impares, es decir, si y lo si todos los e_i son pares, que es lo mismo que decir que n es un cuadrado.

13. **Si n es un cuadrado, demostrar que $d(n)$ es impar**.

    Si n es un cuadrado, todos los exponentes de su descomposición factorial son pares: $n = p_1^{2e_1} \cdots p_r^{2e_r}$. Por tanto $d(n) = (2e_1 + 1) \cdots (2e_r + 1)$ es un producto de números impares y es impar.

14. **Si $d(n)$ es impar, demostrar que n es un cuadrado**.

    Sea $n = p_1^{e_1} \cdots p_r^{e_r}$ tal que $d(n) = (e_1+1) \cdots (e_r+1)$ es impar. Todos los paréntesis deben ser impares, pues si uno de ellos fuera par, también lo sería $d(n)$, así que todos los e_i son pares y n es un cuadrado.

15. **Observar que $1 + \frac{1}{3} = \frac{4}{3}$, $1 + \frac{1}{2} + \frac{1}{4} = \frac{7}{4}$, $1 + \frac{1}{5} = \frac{6}{5}$, $1 + \frac{1}{2} + \frac{1}{3} + \frac{1}{6} = \frac{12}{6}$, $1 + \frac{1}{7} = \frac{8}{7}$ y $1 + \frac{1}{2} + \frac{1}{4} + \frac{1}{8} = \frac{15}{8}$. Enunciar y demostrar un teorema**.

    Las fracciones que sumamos en la parte izquierda de las igualdades son los inversos de los divisores del número. El resultado es una fracción con

numerador la suma de divisores del número y denominador el número. Entonces, el enunciado sería

$$\sum_{d|n} \frac{1}{n} = \frac{\sum\limits_{d|n} d}{n} = \frac{\sigma(n)}{n}.$$

La demostración es sencilla, si tenemos en cuenta que si ordenamos los divisores $d_1 = 1,\ d_2, \ldots, d_{r-1}, d_r = n$ de n cumplen que $d_1 \cdot d_n = d_2 \cdot d_{r-1} = \cdots = n$, y entonces

$$\sum_{d|n} \frac{1}{n} = \frac{1}{d_1} + \frac{1}{d_2} + \cdots \frac{1}{d_{r-1}} + \frac{1}{d_r} = \frac{d_r}{n} + \frac{d_{r-1}}{n} + \cdots + \frac{d_2}{n} + \frac{d_1}{n} = \frac{\sigma(n)}{n}.$$

16. **Encontrar infinitos números n tales que $\sigma(n) \leq \sigma(n-1)$.**

Empecemos por demostrar que hay infinitos primos de la forma $4m+3$. Si hubiera un número finito de ellos, digamos $p_1, p_2, \ldots, p_r$, consideramos el número $n = 4(p_1 p_2 \ldots p_r) - 1 = 4(p_1 p_2 \ldots p_r - 1) + 3$. El número n, que debe ser compuesto, no puede tener todos sus factores primos de la forma $4m+1$, ya que también lo sería n. Entonces, alguno de los primos p_i debe ser factor de n, pero esto es imposible, ya que p_i sería un divisor de 1 por la relación $4p_1 p_2 \ldots p_r - N = 1$.

Ahora, sea n cualquier número primo de la forma $p = 4m+3$. Como n es primo, $\sigma(p) = p+1 = 4m+4$. Por otro lado, $\sigma(p-1) = \sigma(4m+2) = \sigma(2 \cdot (2m+1)) = 3 \cdot \sigma(2m+1) > 3(2m+2) = 6m+6 > 4m+4$.

La solución de este problema no se me ocurrió a mí; después de pensar en números de la forma $n = 2^k + 1$, que también parecen ser solución del problema, pero que no lo pude demostrar, envié un correo a Underwood Dudley pidiendo una pista y esto fue lo que me contestó:

> I don't remember what I had in mind when I first included problem 7 of section 16, but it looks as if taking $n = p$, where p is a prime such that $p = 2s+1$ with s odd works. Then $\sigma(n) = p+1 = 2s+2$, and $\sigma(n-1) = \sigma(2s) = 3 \cdot \sigma(s) \geq 3(s+1) = 3s+3 \geq 2s+2$. The existence of infinitely many such primes is guaranteed by Dirchlet's theorem on primes in arithmetic progressions.

Para no usar el teorema de Dirichlet, lo que he hecho aquí es incluir la demostración del caso particular del teorema de Dirichlet para los primos de la forma $4m+3$.

17. **Si N es impar, ¿cuántas soluciones tiene $x^2 - y^2 = N$?**

Teniendo en cuenta que $x^2 - y^2 = (x+y)(x-y)$, para cada descomposición $N = m \cdot n$, estudiamos el sistema

$$\begin{cases} x + y = m \\ x - y = n \end{cases}.$$

Al ser N impar, también lo serán m y n, y el sistema tendrá una única solución entera, de la forma $x = \frac{1}{2}(m+n)$, $y = \frac{1}{2}(m-n)$. Más aún, suponiendo que

$$(\frac{1}{2}(m_1 + n_1), \frac{1}{2}(m_1 - n_1)) = (\frac{1}{2}(m_2 + n_2), \frac{1}{2}(m_2 - n_2)),$$

fácilmente llegamos a $m_1 = m_2$ y $n_1 = n_2$, es decir, cada sistema produce soluciones diferentes. ¿Cuantas descomposiciones $N = m \cdot n$ podemos hacer? Si sólo contamos los m y n positivos, habrá la mitad de $d(N)$, pero si contamos las posibilidades negativas, el resultado es $2 \cdot d(N)$.

18. **Desarrollar una fórmula para $\sigma_2(n)$, la suma de los cuadrados de los divisores positivos de n.**

Sea $n = p_1^{e_1} \cdots p_r^{e_r}$. Entonces:

$$\begin{aligned} \sigma_2(n) &= \sum_{d|n} d^2 = \sum_{f_i \leqslant e_i} p_1^{2f_1} \cdots p_r^{2f_r} = \sum_{f_1 \leqslant e_1} p_1^{2f_1} \cdots \sum_{f_r \leqslant e_r} p_r^{2f_r} = \\ &= \sum_{f_1 \leqslant e_1} (p_1^2)^{f_1} \cdots \sum_{f_r \leqslant e_r} (p_r^2)^{f_1} = \frac{p_1^{2e_1+1} - 1}{p_1^2 - 1} \cdots \frac{p_r^{2e_r+1} - 1}{p_r^2 - 1}. \end{aligned}$$

19. **Adivinar una fórmula para**

$$\sigma_k(n) = \sum_{d|n} d^k,$$

siendo k un entero positivo.

$$\begin{aligned} \sigma_k(n) &= \sum_{d|n} d^k = \sum_{f_i \leqslant e_i} p_1^{kf_1} \cdots p_r^{kf_r} = \sum_{f_1 \leqslant e_1} p_1^{kf_1} \cdots \sum_{f_r \leqslant e_r} p_r^{kf_r} = \\ &= \sum_{f_1 \leqslant e_1} (p_1^k)^{f_1} \cdots \sum_{f_r \leqslant e_r} (p_r^k)^{f_1} = \frac{p_1^{ke_1+1} - 1}{p_1^k - 1} \cdots \frac{p_r^{ke_r+1} - 1}{p_r^k - 1}. \end{aligned}$$

20. **Demostrar que el producto de los divisores positivos de n es $n^{d(n)/2}$.**

Ordenamos los divisores $d_1 = 1,\ d_2, \ldots, d_{r-1}, d_r = n$ de n de manera que

$$\begin{cases} d_1 d_r = n \\ d_2 d_{r-1} = n \\ \ldots = \ldots \\ d_{r-1} d_2 = n \\ d_r d_1 = n \end{cases}$$

Al multiplicar, obtenemos $(d_1 d_2 \cdots d_{r-1} d_r)^2 = n^{d(n)}$, de donde

$$d_1 d_2 \cdots d_{r-1} d_r = \sqrt{n^{d(n)}} = n^{d(n)/2}.$$

8. Números perfectos

- Un número N es perfecto cuando la suma de todos sus divisores es $2N$, es decir, si es N la suma de sus divisores menores que N.
- Si $2^k - 1$ es primo, entonces $N = 2^{n-1}(2^k - 1)$ es primo.
- Si N es par y perfecto, entonces $N = 2^{p-1}(2^p - 1)$ para algún primo p y $2^p - 1$ también es primo.
- M y N son amigos cuando $\sigma(M) = \sigma(N) = M + N$.
- N abundante si $\sigma(n) > 2n$, deficiente si $\sigma(n) < 2n$ y triangular si es de la forma $\frac{1}{2}n(n+1)$.

1. **Comprobar que** $2620, 2924$ **y** $17296, 18416$ **son parejas de números amigos. (La última pareja, descubierta por Fermat, fue la segunda encontrada. Tener en cuenta que** $17296 = 2^4 \cdot 23 \cdot 47$ **y** $18416 = 2^4 \cdot 1151$**).**

   Con `Divisors[2620]`, *Mathematica* nos dice que los divisores de 2620 son 1, 2, 4, 5, 10, 20, 131, 262, 524, 655, 1310, 2620. Usando ahora la isntrucción `DivisorSigma[1,2620]` obtenemos que la suma de estos divisores es $\sigma(2620) = 5544$.

   De forma parecida, obtenemos que los divisores de 2924 son 1, 2, 4, 17, 34, 43, 68, 86, 172, 731, 1462, 2924, siendo su suma también igual a 5544. Por tanto 2620 y 2924 son números amigos.

   Con 17296 y 18416, hay más números:

   - Divisores de 17296: 1, 2, 4, 8, 16, 23, 46, 47, 92, 94, 184, 188, 368, 376, 752, 1081, 2162, 4324, 8648, 17296.
   - Divisores de 18416: 1, 2, 4, 8, 16, 1151, 2302, 4604, 9208, 18416.
   - Suma de los divisores, en ambos casos: 35712.

   Por tanto, también se trata de números amigos.

2. **Durante largo tiempo se pensó que los números perfectos terminaban alternativamente en 6 y 8. Demostrar que esto no es correcto comprobando que los números correspondientes a los primos** $2^{13} - 1$ **y** $2^{17} - 1$ **acaban ambos en 6**.

Sea $p = 13$ o $p = 17$. El número perfecto correspondiente es $N = 2^{p-1}(2^p - 1)$. Como p es de la forma $4m + 1$, 2^p acaba en 2 y $2^p - 1$ acaba en 1. Ahora, $p - 1$ es múltiplo de 4 y 2^{p-1} acaba en 6, por lo que N acabará en 6.

3. **Clasificar los enteros** $2, 3, \ldots, 21$ **como abundantes, deficientes o perfectos**.

   6 es perfecto. 12, 18 y 20 son abundantes. Los demás, 2, 3, 4, 5, 7, 8, 9, 10, 11, 13, 14, 15, 16, 17, 19 y 21, son deficientes.

4. **Clasificar los enteros** $402, 403, \ldots, 421$ **como abundantes, deficientes o perfectos**.

   402, 408, 414, 416 y 420 son abundantes. El resto, 403, 404, 405, 406, 407, 409, 410, 411, 412, 413, 415, 417, 418, 419 y 421 son deficientes.

n	402	403	404	405	406	407	408	409	410	411
$\sigma(n)$	816	448	714	726	720	456	1080	410	756	552

n	412	413	414	415	416	417	418	419	420	421
$\sigma(n)$	728	480	936	504	882	560	720	420	1344	422

5. **Si** $\sigma(n) = kn$**, se dice que** n **es un *número k-perfecto*. Comprobar que** 672 **es 3-perfecto y que** $2,178,540 = 2^2 \cdot 3^2 \cdot 5 \cdot 7^2 \cdot 13 \cdot 19$ **es 4-perfecto**.

   $672 = 2^5 \cdot 3 \cdot 7$. A partir de aquí obtenemos:

   $$\sigma(672) = (2^6 - 1) \cdot (3 + 1) \cdot (7 + 1) = 63 \cdot 32 = 2016 = 3 \cdot 672.$$

   $$\begin{aligned}\sigma(2178540) =& (1 + 2 + 2^2) \cdot (1 + 3 + 3^2) \cdot 6 \cdot (1 + 7 + 7^2) \cdot 14 \cdot 20 = \\ =& 7 \cdot 13 \cdot 6 \cdot 57 \cdot 14 \cdot 20 = \\ =& 8714160 = 4 \cdot 2178540.\end{aligned}$$

6. **Demostrar que no hay números de la forma** $2^a 3^b$ **que sean 3-perfectos**.

   Supongamos que $N = 2^a 3^b$ es 3-perfecto. Entonces $de\sigma(N) = 3N$ deducimos que

   $$(2^{a+1} - 1) \cdot \frac{3^{a+1} - 1}{2} = 2^a 3^{a+1} \Rightarrow (2^{a+1} - 1)(3^{a+1} - 1) = 2^{a+1} 3^{a+1}.$$

Multiplicando y cancelando, obtenemos $2^{a+1} + 3^{a+1} = 1$, que es imposible.

7. **Diremos que un número n es *superperfecto* si $\sigma(\sigma(n)) = 2n$. Demostrar que si $n = 2^k$ y $2^{k+1} - 1$ es primo, entonces n es superperfecto**.

   Con las hipótesis sobre n, es evidente que

   $$\sigma(\sigma(n)) = \sigma(\sigma(2^k)) = \sigma(2^{k+1} - 1) = 2^{k+1} = 2n.$$

8. **Durante mucho tiempo se pensó que todo número abundante era par. Demostrar que 945 es abundante, y encontrar otro número abundante de la forma $3^a \cdot 5 \cdot 7$.**

   Como $945 = 3^2 \cdot 109$,
   $\sigma(945) = (1 + 3 + 3^2) \cdot (1 + 109) = 13 \cdot 110 = 1430 > 945$.

   Si $n = 3^a \cdot 5 \cdot 7$, entonces $\sigma(n) = \frac{3^{a+1}-1}{2} \cdot 6 \cdot 8 = 24(3^{a+1} - 1) = 72 \cdot 3^a - 24$. Entonces $\sigma(n) > n \Leftrightarrow 72 \cdot 3^a - 24 > 35 \cdot 3^a \Leftrightarrow 37 \cdot 3^a > 35 \Leftrightarrow a \geq 0$. Es decir, todos los números de la forma $3^a \cdot 5 \cdot 7$ son abundantes.

9. **En 1575 se observó que todo número perfecto par es un número triangular. Demostrar que esto es así**.

   Sea N un número perfecto par. Por el teorema de Euler, N es de la forma $2^{k-1}(2^{k-1} - 1)$, siendo $2^{k-1} - 1$ primo. Entonces $N = 2^{k-1}(2^k - 1) = \frac{1}{2}(2^k - 1)2^k$, es decir N es de la forma $\frac{1}{2}m(m+1)$ con $m = 2^k - 1$ y es un número triangular.

10. **En 1575 se observó que**

    $$\begin{aligned} 6 &= 1 + 2 + 3, \\ 28 &= 1 + 2 + 3 + \cdots + 7, \\ 496 &= 1 + 2 + 3 + \cdots + 31. \end{aligned}$$

    ¿Puede esto continuar?

    Según hemos visto en el ejercicio anterior, cualquier número perfecto par es un número triangular:

    $$2^{k-1}(2^k - 1) = \frac{1}{2}(2^k - 1)2^k = 1 + 2 + 3 + \cdots + (2^k - 1).$$

11. **Sean**

$$\begin{aligned} p =& 3 \cdot 2^e - 1, \\ q =& 3 \cdot 2^{e-1} - 1, \\ r =& 3^2 \cdot 2^{2e-1} - 1, \end{aligned}$$

siendo e un entero positivo. Si p, q y r son primos, demostrar que $2^e pq$ y $2^e r$ son amigos. (Considerando $e \leq 200$, p, q y r son primos sólo para $e = 2, 4, 7$.)

Sean $M = 2^e pq$, $N = 2^e r$.

$$\begin{aligned} \sigma(M) =& \sigma(2^e pq) = (2^{e+1} - 1)(p+1)(q+1) = \\ =& (2^{e+1} - 1) \cdot 3 \cdot 2^e \cdot 3 \cdot 2^{e-1} = \\ =& 2^{2e-1} \cdot 3^2 \cdot (2^{e+1} - 1). \\ \sigma(N) =& \sigma(2^e r) = (2^{e+1} - 1)(r+1) = (2^{e+1} - 1) \cdot 3^2 \cdot 2^{2e-1}. \end{aligned}$$

Habiendo comprobado que $\sigma(M) = \sigma(N)$, sólo queda ver que ambos valores de σ son iguales a $M + N$ para demostrar que M y N son amigos:

$$\begin{aligned} M + N =& 2^e(pq + r) = \\ =& 2^e \left((3 \cdot 2^e - 1) \cdot (3 \cdot 2^{e-1} - 1) + (3^2 \cdot 2^{2e-1} - 1) \right) = \\ =& 2^e (3^2 \cdot 2^{2e-1} - 3 \cdot 2^e - 3 \cdot 2^{e-1} + 1 + 3^2 \cdot 2^{2e-1} - 1) = \\ =& 2^e (2 \cdot 3^2 \cdot 2^{2e-1} - 9 \cdot 2^{e-1}) = \\ =& 2^e \cdot 3^2 \cdot (2^{2e} - 2^{e-1}) = 2^{2e-1} \cdot 3^2 \cdot (2^{e+1} - 1). \end{aligned}$$

El programita siguiente nos permite confirmar la afirmación del enunciado:

```
For[e = 1, e <= 2000, e++,
  p := 3*2^e - 1;
  q := 3*2^(e - 1) - 1;
  r := 3^2 2^(2 e - 1) - 1;
  If[PrimeQ[p] && PrimeQ[q] && PrimeQ[r],
    Print[{e, p, q, r, 2^e p q, 2^e r}]]]
```

e	p	q	r	M	N
2	11	5	71	220	284
4	47	23	1151	17296	18416
7	383	191	73727	9363584	9437056

12. **Demostrar que si $p > 3$ y $2p + 1$ es primo, entonces $2p(2p + 1)$ es deficiente**.

Sea $n = 2p(2p + 1)$. Suponiendo, que no lo dice el enunciado, que p es primo, tenemos $\sigma(p) = 3(p+1)(2p+2) = 6(p+1)^2 = 6p^2+12p+6$. Por otro lado, $2n = 4p(2p+1) = 8p^2+4p$ y $6p^2+12p+6 < 8p^2+4p \Leftrightarrow 2p^2-8p-6 > 0 \Leftrightarrow p^2-4p-3 > 0 \Leftrightarrow p^2-4p+4 > 1 \Leftrightarrow (p-2)^2 > 1 \Leftrightarrow p > 3$.

La suposición de que p sea primo, que el autor habrá considerado implícita al llamar p al número es necesaria para concluir que el n es deficiente, pues si tomamos $p = 6$, $n = 156 = 2^2 \cdot 3 \cdot 13$ y $\sigma(156) = (1 + 2 + 4) \cdot 4 \cdot 14 = 392 > 312 = 2 \cdot 156$.

13. **Demostrar que todos los números perfectos pares acaban en 6 o en 8**.

Sabemos que un número perfecto par es de la forma $2^{p-1}(2^p-1)$, siendo p un número primo.

Si p es de la forma $4k+1$, entonces $n = 2^{4k}(2^{4k+1}-1) = 16^k \cdot (2 \cdot 16^k - 1)$. Como 16^k siempre acaba en 6 y $2 \cdot 16^k - 1$ siempre acaba en 1, n acabará en 6.

Supongamos ahora que p es de la forma $4k + 3$.
Entonces $n = 2^{4k+2}(2^{4k+3} - 1) = 4 \cdot 16^k \cdot (8 \cdot 16^k - 1)$. Como $4 \cdot 16^k$ siempre acaba en 4 y $8 \cdot 16^k - 1$ siempre acaba en 7, n acabará en 8.

14. **Si n es un número perfecto par y $n > 6$, demostrar que la suma de sus dígitos es congruente con 1 (mód 9)**.

Sabemos que un número perfecto par es de la forma $2^{p-1}(2^p-1)$, siendo p un número primo.

- Si p es de la forma $4k + 1$, entonces $n = 2^{4k}(2^{4k+1} - 1)$. Consideremos los diferentes casos de k módulo 3 en la siguiente tabla:

k (mód 3)	2^{4k} (mód 9)	$(2^{4k+1} - 1)$ (mód 9)
0	1	1
1	7	4
2	4	7

Vemos que en todos los casos es $2^{4k} \cdot (2^{4k+1} - 1) \equiv 1$ (mód 9).

- Si p es de la forma $4k+3$, entonces $n = 2^{4k+2}(2^{4k+3}-1)$. Distinguiendo casos como antes tenemos:

k (mód 3)	2^{4k+2} (mód 9)	$(2^{4k+3}-1)$ (mód 9)
0	4	7
1	1	1
2	7	4

  También aquí es $2^{4k} \cdot (2^{4k+1}-1) \equiv 1$ (mód 9) en todos los casos.

15. **Si p es impar, demostrar que** $2^{p-1}(2^p-1) \equiv 1+\frac{9}{2}p(p-1)$ **(mód** 81).

9. El teorema y la función de Euler

1. **Calcular** $\phi(42)$**,** $\phi(420)$ **y** $\phi(4200)$.

$$\begin{aligned}\phi(42) =&\phi(2\cdot 3\cdot 7) = \phi(2)\cdot\phi(3)\cdot\phi(7) = 1\cdot 2\cdot 6 = 12.\\ \phi(420) =&\phi(2^2\cdot 3\cdot 5\cdot 7) = \phi(2^2)\cdot\phi(3)\cdot\phi(5)\cdot\phi(7) =\\ =&(2^2-2)\cdot 2\cdot 4\cdot 6 = 96.\\ \phi(4200) =&\phi(2^3\cdot 3\cdot 5^2\cdot 7) = \phi(2^3)\cdot\phi(3)\cdot\phi(5^2)\cdot\phi(7) =\\ =&(2^3-2^2)\cdot 2\cdot(5^2-5)\cdot 6 = 960.\end{aligned}$$

2. **Calcular** $\phi(54)$**,** $\phi(540)$ **y** $\phi(5400)$.

$$\begin{aligned}\phi(54) =&\phi(2\cdot 3^3) = \phi(2)\cdot\phi(3^3) = 1\cdot(3^3-3^2) = 18.\\ \phi(540) =&\phi(2^2\cdot 3^3\cdot 5) = \phi(2^2)\cdot\phi(3^3)\cdot\phi(5) =\\ =&(2^2-2)\cdot(3^3-3^2)\cdot(5-1) = 2\cdot 18\cdot 4 = 144.\\ \phi(5400) =&\phi(2^3\cdot 3^3\cdot 5^2) = \phi(2^3)\cdot\phi(3^3)\cdot\phi(5^2) =\\ =&(2^3-2^2)\cdot(3^3-3^2)\cdot(5^2-5) = 1440.\end{aligned}$$

3. **Calcular** ϕ **para** $10115 = 5\cdot 7\cdot 17^2$ **y** $100115 = 5\cdot 20023$.

$$\begin{aligned}\phi(10115) =&\phi(5\cdot 7\cdot 17^2) = \phi(5)\cdot\phi(7)\cdot\phi(17^2) =\\ =&4\cdot 6\cdot(17^2-17) = 4\cdot 6\cdot 17\cdot 16 = 6528.\\ \phi(100115) =&\phi(5\cdot 20023) = \phi(5)\cdot\phi(20023) = 4\cdot 20022 = 80088.\end{aligned}$$

4. **Calcular** ϕ **para** $10116 = 2^2\cdot 3^2\cdot 281$ **y** $100116 = 2^2\cdot 3^5\cdot 103$.

$$\begin{aligned}\phi(10116) =&\phi(2^2\cdot 3^2\cdot 281) = \phi(2^2)\cdot\phi(3^2)\cdot\phi(281) =\\ =&(2^2-2)\cdot(3^2-3)\cdot(281-1) = 2\cdot 6\cdot 280 = 3360.\\ \phi(100116) =&\phi(2^2\cdot 3^5\cdot 103) = \phi(2^2)\cdot\phi(3^5)\cdot\phi(2^2\cdot 3^5\cdot 103) =\\ =&(2^2-2)\cdot(3^5-3^4)\cdot 102 = 33048.\end{aligned}$$

5. **Calcular** a^8 **(mód** 15**) para** $a = 1, 2, \ldots, 14$.

a	1	2	3	4	5	6	7	8	9	10	11	12	13	14
a^2	1	4	9	1	10	6	4	4	6	10	1	9	4	1
a^4	1	1	6	1	10	6	1	1	6	10	1	6	1	1
a^8	1	1	6	1	10	6	1	1	6	10	1	6	1	1

(Se puede comprobar con `Table[Mod[a^8, 15], {a, 1, 14}]`) $\boxed{\mathcal{M}}$

6. **Calcular a^8 (mód 16) para $a = 1, 2, \ldots, 15$.**

a	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
a^2	1	4	9	0	9	4	1	0	1	4	9	0	9	4	1
a^4	1	0	1	0	1	4	1	0	1	0	1	0	1	0	1
a^8	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1

(Se puede comprobar con `Table[Mod[a^8, 16], {a, 1, 15}]`). $\boxed{\mathcal{M}}$

7. Demostrar que si n es impar, entonces $\phi(4n) = 2n$.

   $\phi(4) = \phi(2^2) = 2^2 - 2 = 2$. Entonces, al ser ϕ una función multiplicativa, $\phi(4n) = \phi(4)\phi(n) = 2\phi(n)$.

8. Los números perfectos cumplen $\sigma(n) = 2n$. ¿Qué números cumplen $\phi(n) = 2n$?

   Ninguno, ya que para cualquier n es $\phi(n) < n < 2n$.

9. $1 + 2 = \frac{3}{2}\phi(3)$, $1 + 3 = \frac{4}{2}\phi(4)$, $1 + 2 + 3 + 4 = \frac{5}{2}\phi(5)$, $1 + 5 = \frac{6}{2}\phi(6)$, $1 + 2 + 3 + 4 + 5 + 6 = \frac{7}{2}\phi(7)$, $1 + 3 + 5 + 7 = \frac{8}{2}\phi(8)$. **Enunciar un teorema.**

   Todos los sumandos que vemos son primos relativos con n y menores que n: *La suma de los números primos relativos con n y menores que n es* $\frac{n}{2}\phi(n)$. Es decir:

$$\sum d = \frac{n}{2}\phi(n),$$

   donde la suma se efectúa sobre los números primos relativos con n y menores que n.

   Teniendo en cuenta que hay $\phi(n)$ divisores de n y menores que n, podemos expresar:

$$\sum d = \tfrac{n}{2}\sum 1 \Leftrightarrow \sum \left(d - \tfrac{n}{2}\right) = 0 \Leftrightarrow \sum (2d - n) = 0.$$

   Si $1 \leq d < n$ es primo relativo con n, también lo es $d' = n - d$. Teniendo en cuenta que $2d' - n = 2(n - d) - n = n - 2d$, la suma anterior estará formada por pares de sumandos opuestos que se cancelarán y darán resultado 0.

10. **Demostrar que**

$$\sum_{p\le x}\sigma(p)-\sum_{p\le x}\phi(p)=\sum_{p\le x}d(p).$$

Si p es primo, $\sigma(p)=p+1$, $\phi(p)=p-1$ y $d(p)=2$, por lo que, para cada p se cumple que $\sigma(p)-\phi(p)=d(p)$.

11. **Demostrar el Lema 3, es decir que si** $(a,m)=1$ **y** $a\equiv b$ **(mód** m**), entonces** $(b,m)=1$**, usando para ello que existen enteros** r **y** s **tales que** $ax+my=1$.

En efecto, la condición $(a,m)=1$ implica que existen enteros r y s tales que $ax+my=1$. Por su parte, la condición $a\equiv b\ (\text{mód } m)$ implica que existe un entero k tal que $a-b=km$. Sustituyendo $a=b+km$ en $ax+my=1$, obtenemos $(b+km)x+my=1$, es decir, $bx+m(kx+y)=1$, es decir, existen números enteros $x'=x$, $y'=kx+y$ tales que $bx'+my'=1$, por lo que $(b,m)=1$.

12. **Si** $(a,m)=1$**, demostrar que cualquier** x **cumpliendo la congruencia** $x\equiv ca^{\phi(m)-1}$ **(mód** m**) cumple** $ax\equiv c$ **(mód** m**).**

$x\equiv ca^{\phi(m)-1}\ (\text{mód } m)\Rightarrow ax\equiv aca^{\phi(m)-1}=ca^{\phi(m)}\equiv c\ (\text{mód } m)$.

13. **Sea** $f(n)=(n+\phi(n))/2$**. Demostrar que** $f(f(n))=\phi(n)$ **si** $n=2^k$**,** $k=2,3,\ldots$.

$$\begin{aligned}\phi(n)=&\phi(2^k)=2^k-2^{k-1}=2^{k-1}\\ f(n)=&\frac{n+\phi(n)}{2}=\frac{2^k+2^{k-1}}{2}=2^{k-1}+2^{k-2}=3\cdot 2^{k-2}\\ f(f(n))=&\frac{3\cdot 2^{k-2}+2\cdot(2^{k-2}-2^{k-3})}{2}=\frac{3\cdot 2^{k-2}+2^{k-1}-2^{k-2}}{2}=\\ =&2\cdot 2^{k-2}=2^{k-1}=\phi(n).\end{aligned}$$

14. **Encontrar cuatro soluciones de** $\phi(n)=16$.

Una primera solución es $n=17$, pues 17 es primo y $\phi(n)=17-1=16$. Otra solución fácil es $n=2^5=32$, puesto que $\phi(2^k)=2^{k-1}$ y $16=2^4$. Pongamos $n=2^ep$ con p primo. Entonces $\phi(n)=2^{e-1}(p-1)=16$.

Dando valores a e obtenemos soluciones para $p = \frac{16}{2^{e-1}} + 1$ y $n = 2^e p$:

$$\begin{aligned} e = 1, &\quad p = 17, \quad n = 34 \\ e = 3, &\quad p = 5, \quad n = 40 \\ e = 4, &\quad p = 3, \quad n = 48 \end{aligned}$$

¿Habrá más soluciones? Si preguntamos a *Mathematica* con
`For[n=1, n<=100, n++, If[EulerPhi[n]==16,Print[n]]]` $\boxed{\mathcal{M}}$

A parte de las cinco soluciones anteriores, nos dará $n = 60$.

15. **Encontrar todas las soluciones de $\phi(n) = 4$ y demostrar que no hay más**.

Si n es impar, no puede tener factores de la forma m^2, pues entonces m sería un factor de $\phi(m) = 4$. Como los divisores de 4 son sólo 1, 2 y 4, los factores impares de n sólo pueden ser 3 y 5. Pero $n = 3s \Rightarrow 4 = \phi(n) = 2\phi(s) \Rightarrow \phi(s) = 2 \Rightarrow s = 3$. (imposible). Por tanto la única posibilidad cuando n es impar es $n = 5$.

Si $n = 2^e$, $\phi(n) = 2^{e-1} = 4 \Rightarrow e = 3 \Rightarrow n = 8$.

Si $n = 2^e m$, con m impar, $\phi(n) = 2^{e-1}\phi(m) = 4$.

$$\begin{aligned} e = 1, &\quad \phi(m) = 4, \quad m = 5, \quad n = 10 \\ e = 2, &\quad \phi(m) = 2, \quad m = 3, \quad n = 12 \\ e = 4, &\quad \phi(m) = 1, \quad \text{imposible} \end{aligned}$$

Las soluciones, son por tanto, 5, 8, 10 y 12.

16. **Demostrar que $\phi(mn) > \phi(m)\phi(n)$ si m y n tienen un factor común mayor que 1**.

Si $(m, n) = d$, entonces $m = dm'$ y $n = dn'$ con $(m', n') = 1$. Llamemos $d_1 = (d, m')$ y $d_2 = (d, n')$.

17. **Demostrar que $(m, n) = 2$ implica $\phi(mn) = 2\phi(m)\phi(n)$.**

Podemos escribir $m = 2^r u$, $n = 2^s v$, siendo exactamente uno de los números r y s igual a 1, y siendo también u y v números impares tales que $(u, v) = 1$. Con todo ello podemos calcular

$$\begin{aligned} &\phi(m) = 2^{r-1}\phi(u), \\ &\phi(n) = 2^{s-1}\phi(v), \\ &\phi(mn) = \phi(2^{r+s}uv) = 2^{r+s-1}\phi(uv), \\ &\phi(m)\phi(n) = 2^{r-1}\phi(u)2^{s-1}\phi(v) = 2^{r+s-2}\phi(uv). \end{aligned}$$

18. **Demostrar que $\phi(n) = \frac{n}{2}$ si y solo si $n = 2^k$ para algún entero positivo k.**

La parte evidente es que si $n = 2^k$, entonces

$$\phi(n) = 2^{k-1}(2-1) = 2^{k-1} = \frac{n}{2}.$$

Ahora supongamos que $\phi(n) = \frac{n}{2}$. Como n es par, será de la forma $n = 2^k m$ con m impar. Entonces

$$2^{k-1}m = \frac{n}{2} = \phi(n) = \phi(2^k m) = 2^{k-1}\phi(m) \Rightarrow \phi(m) = m \Rightarrow m = 1,$$

resultando n un número de la forma 2^k para algún entero positivo k.

19. **Demostrar que $n-1$ y $n+1$ son ambos primos y $n > 4$ entonces $\phi(n) \leq \frac{n}{3}$.**

Si $n-1$ y $n+1$ son primos, desde luego n es par, y además es divisible por 3, y puede expresarse $n = 2^k 3^h m$ con $(2, m) = (3, m) = 1$ y $k, h \geq 1$. Entonces, $\phi(n) = 2^{k-1} \cdot 3^{h-1} \cdot 2 \cdot \phi(m) = 2^k \cdot 3^{h-1} \cdot \phi(m) \leq 2^k 3^{h-1} m = \frac{n}{3}$.

20. **Demostrar que $\phi(n) = 14$ es imposible.**

Si p^e es la mayor potencia de un primo p que divide a n, entonces $p^{e-1}(p-1)$ divide a $\phi(n) = 14$. Entonces, $p-1$ puede ser 1, 2, 7 o 14. Como p es primo, p puede ser únicamente 2 o 3. El caso $p = 3$ obliga a que $e \leq 1$ y en el caso $p = 2$ puede ser $e \leq 2$. Entonces $n = 2^e 3^f$ siendo $0 \leq e \leq 2$ y $0 \leq f \leq 1$. Los valores posibles para n se reducen a 1, 2, 3, 4, 6, 12 y los correspondientes valores de $\phi(n)$ son 1, 1, 2, 2, 2, 4.

10. Raíces primitivas

1. **Encontrar los órdenes de** $1, 2, \ldots, 12$ **(mód** 13**).**

   Construimos la siguiente tabla:

a	1	2	3	4	5	6	7	8	9	10	11	12
a^2		4	9	3	12	10	10	12	3	9	4	1
a^3		8	1	12	8	8	5	5	1	12	5	
a^4		3		9	1	9	9	1		3	3	
a^5		6		10		2	11			4	7	
a^6		12		1		12	12			1	12	
a^7		11				7	6				2	
a^8		9				3	3				9	
a^9		5				5	8				8	
a^{10}		10				4	4				10	
a^{11}		7				11	2				6	
a^{12}		1				1	1				1	
$o(a)$	1	12	3	6	4	12	12	4	3	6	12	2

2. **Encontrar los órdenes de** $1, 2, \ldots, 16$ **(mód** 17**).**

   Construimos la siguiente tabla:

a	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
a^2		4	9	16	8	2	15	13	13	15	2	8	16	9	4	1
a^3		8	10	13	6	12	3	2	15	14	5	11	4	7	9	
a^4		16	13	1	13	4	4	16	16	4	4	13	1	13	16	
a^5		15	5		14	7	11	9	8	6	10	3		12	2	
a^6		13	15		2	8	9	4	4	9	8	2		15	13	
a^7		9	11		10	14	12	15	2	5	3	7		6	8	
a^8		1	16		16	16	16	1	1	16	16	16		16	1	
a^9			14		12	11	10			7	6	5		3		
a^{10}			8		9	15	2			2	15	9		8		
a^{11}			7		11	5	14			3	12	6		10		
a^{12}			4		4	13	13			13	13	4		4		
a^{13}			12		3	10	6			11	7	14		5		
a^{14}			2		15	9	8			8	9	15		2		
a^{15}			6		7	3	5			12	14	10		11		
a^{16}			1		1	1	1			1	1	1		1		
$o(a)$	1	8	16	4	16	16	16	8	8	16	16	16	4	16	8	2

3. **Una de las raíces primitivas de** 19 **es** 2**. Encontrar todas las demás**.

   Por ser 2 una raíz primitiva de 19, sabemos que 2^k es una raíz primitiva módulo de 19 si y solo si $(k, 18) = 1$:

k	1	5	7	11	13	17
2^k	2	13	14	15	3	10

4. **Una de las raíces primitivas de** 23 **es** 5**. Encontrar todas las demás**.

   Por ser 5 una raíz primitiva de 23, sabemos que 5^k es una raíz primitiva módulo de 23 si y solo si $(k, 22) = 1$:

k	1	3	5	7	9	13	15	17	19	21
5^k	5	10	20	17	11	21	19	15	7	14

5. **¿Cuáles son los órdenes de 2, 4, 7, 8, 11, 13 y 14 (mód** 15**)?. ¿Tiene 15 raíces primitivas?**

a	2	4	7	8	11	13	14
a^2	4	1	4	4	1	4	1
a^3	8		13	2		7	
a^4	1		1	1		1	
$o(a)$	4	2	4	4	2	4	2

   Vemos que en ningún caso es $o(a) = \phi(15) = 10$. Por tanto, 15 no tiene raíces primitivas.

6. **¿Cuáles son los órdenes de 3, 7, 9, 11, 13, 17 y 19 (mód** 20**)?. ¿Tiene 20 raíces primitivas?**

a	3	7	9	11	13	17	19
a^2	9	9	1	1	9	9	1
a^3	7	3			17	13	
a^4	1	1			1	1	
$o(a)$	4	4	2	2	4	4	2

   Vemos que en ningún caso es $o(a) = \phi(20) = 8$. Por tanto, 20 no tiene raíces primitivas.

7. **¿Qué enteros tienen orden 6 (mód 31)?.**

   Como $6|(31-1)$, sabemos que hay $\phi(6) = 2$ restos (mód 31) cuyo orden es 6. Haciendo pruebas, encontramos que uno es $a = 6$: $6^2 = 5$, $6^3 = 30$, $6^4 = 25$, $6^5 = 26$, $6^6 = 1$. El otro, lo podemos encontrar sabiendo que es de la forma 6^k con (k,6)=1, es decir, $6^5 = 26$.

8. **¿Qué enteros tienen orden 6 (mód 37)?.**

   Como $6|(37-1)$, sabemos que hay $\phi(6) = 2$ restos (mód 37) cuyo orden es 6. Haciendo pruebas, encontramos que uno es $a = 11$: $11^2 = 10$, $11^3 = 36$, $11^4 = 26$, $11^5 = 27$, $11^6 = 1$. El otro, lo podemos encontrar sabiendo que es de la forma 11^k con (k,6)=1, es decir, $11^5 = 27$.

9. **Si a, $a \neq 1$, tiene orden t (mód p), demostrar que**

   $$a^{t-1} + a^{t-2} + \cdots + 1 = 0 \text{ (mód } p).$$

   Recordemos la fórmula $a^t - 1 = (a-1)(a^{t-1} + a^{t-2} + \cdots + 1)$. Si a tiene orden t, la parte izquierda es cero módulo p, por lo que p divide a alguno de los paréntesis de la parte derecha, y p no puede dividir a $a - 1$, porque entonces el orden de a sería 1.

10. **Si g y h son dos raíces primitivas de un primo impar p, entonces $g \equiv h^k$ (mód p) para algún entero k. Demostrar que k es impar.**

    Supongamos que k es par. Entonces

    $$g^{\frac{p-1}{2}} = (h^k)^{\frac{p-1}{2}} = (h^{p-1})^{\frac{k}{2}} = 1 \text{ (mód } p),$$

    en contra de que g es una raíz primitiva y $p-1$ es el menor exponente al que tenemos que elevar g para obtener 1 (mód p).

11. **Demostrar que si g y h son raíces primitivas de un primo p, entonces el resto de gh no es una raíz primitiva de p.**

    Según se ha visto en el ejercicio anterior, si gh fuera una raíz primitiva de p, podría expresarse $gh = g^k$ para un cierto k que, además debe ser impar. Pero entonces, tenemos $h = g^{k-1}$, teniendo que ser $k-1$ también impar, lo cual es imposible.

12. **Si g, h y k son raíces primitivas de p, es siempre el resto de ghk una raíz primitiva de p?**

No. Por ejemplo, para $p = 19$, hemos visto en el ejercicio 3 que 2, 3 y 14 son raíces primitivas. Su producto es 8, que no es una raíz primitiva.

13. **Demostrar que si a tiene orden 3 (mód p), entonces $a+1$ tiene orden 6 (mód p).**

Por tener a orden 3 (mód p), cumple $a^3 - 1 \equiv 0$ (mód p). Por tanto, $a^2 + a + 1 \equiv 0$ (mód p) y

$$(a+1)^3 = a^3 + 3a^2 + 3a + 1 \equiv 3(a^2 + a) + 2 \equiv -1 \text{ (mód } p).$$

De aquí $(a+1)^6 \equiv 1$ (mód p) y el orden de $a+1$ debe ser un divisor de 6. El orden de $a+1$ no puede ser 1, pues en ese caso,

$$a + 1 \equiv 1 \text{ (mód } p) \Rightarrow a \equiv -1 \text{ (mód } p) \Rightarrow a^3 \equiv -1 \text{ (mód } p),$$

en contra de la hipótesis. Si el orden de $a+1$ fuera 2, tendríamos

$$(a+1)^2 \equiv 1 \text{ (mód } p) \Rightarrow a^2+2a+1 \equiv 1 \text{ (mód } p) \Rightarrow a^2+2a \equiv 0 \text{ (mód } p),$$

y, teniendo en cuenta que $a^2 + a \equiv -1$ (mód p), nos lleva a $a - 1 \equiv 0$ (mód p), lo cual es imposible si a tiene orden 3. La única posibilidad que queda es que el orden de $a+1$ sea 6.

14. **Si p y q son primos impares y $q|a^p + 1$, demostrar que o $q|a+1$ o $q = 2kp + 1$ para algún entero k.**

Como $q|a^p + 1 \Rightarrow a^p \equiv -1$ (mód p) $\Rightarrow (-a)^p \equiv 1$ (mód p), el orden de $-a$ (mód p), debe ser un divisor de p: 1 ó p. Si el orden de $-a$ es 1, entonces $-a \equiv 1$ (mód p) $\Rightarrow a + 1 \equiv 0$ (mód p) $\Rightarrow p$ divide a $a+1$.

Si el orden de $-a$ es p, entonces, p divide a $q - 1 = \phi(q)$, por lo que $q = 1 + rp$ para algún entero r. Como p y q son impares, r debe ser par, resultando que $q = 1 + 2kp$ para algún entero k.

15. **Suponiendo que a tiene orden 4 (mód p), ¿cuál es el resto de $(a+1)^4$ (mód p)?.**

Como $a^4-1 = (a-1)(a+1)(a^2+1$, obtenemos que $a^2 \equiv -1$ y $a^3 \equiv -a$, por lo que $(a+1)^4 = a^4 + 4a^3 + 6a^2 + 4a + 1 = 1 - 4a - 6 + 4a + 1 = -4 = p - 4$ (mód p).

16. **Demostrar que** $131071 = 2^{17} - 1$ **es primo**.

Como ningún primo impar p divide a $2 - 1$, un primo p que divida a $2^{17} - 1$ debe ser de la forma $2 \cdot 17k + 1 = 34k + 1$. Los valores de $34 + 1$, primos y menores que $\sqrt{131071} \simeq 362{,}07$ son 103, 137, 239, 273, 307. Al dividir 131071 por estos números obtenemos de resto, 55, 99, 99, 31, 289, respectivamente. Por tanto, el número 131071 es primo.

17. **Demostrar que** $(2^{19} + 1)/3$ **es primo**.

Usaremos que si un primo p divide a $2^{19} + 1$, entonces $p|2 + 1$ o p es de la forma $p = 38k + 1$. Los números de la forma $38k + 1$ menores que $\sqrt{174763} \simeq 418{,}047$ son 39, 77, 115, 153, 191, 229, 267, 305, 343, 381, de los cuales son primos sólo 191 y 229. Como al dividir 174763 por estos números obtenemos restos no nulos (189 y 36, respectivamente), el número $(2^{19} + 1)/3$ es primo.

18. **Demostrar que si** g **es una raíz primitiva de** p**, entonces hay dos potencias consecutivas de** g **que tienen restos consecutivos. Es decir, demostrar que existe** k **tal que** $g^{k+1} \equiv g^k + 1$ **(mód** p**)**.

Consideremos los restos de los números de la forma $g^{k+1} - g^k = g^k(g-1)$, $(1 \leq k \leq p - 1)$.

Estos números son todos distintos (mód p): Sea $1 \leq r < s \leq p - 1$ y $g^r(g - 1) \equiv g^s(g - 1)$ (mód p). Entonces $g^r \equiv g^s$ (mód p) y $g^{s-r} \equiv 1$ (mód p), en contra de que g es una raíz primitiva de p.

Como p no divide a ninguno de los números $g^k(g - 1)$, nunca es $g^{k+1} - g^k \equiv 0$ (mód p), por lo que para cada $1 \leq t \leq p - 1$ existirá algún k tal que $g^{k+1} - g^k \equiv t$ (mód p), en particular para $t = 1$, que es lo que queremos probar.

Como ejemplo, consideremos lo que ocurre con $p = 11$ y $g = 6$:

k	1	2	3	4	5	6	7	8	9	10
g^k	6	3	7	9	10	5	8	4	2	1
$g^{k+1} - g^k$	-3	4	2	1	-5	3	-4	-2	-1	5

En este caso tenemos $g^5 = g^4 + 1$ (mód 11).

19. **Demostrar que si g es una raíz primitiva de p, entonces no hay tres potencias consecutivas de g que tengan restos consecutivos. Es decir, demostrar $g^{k+2} \equiv g^{k+1} + 1 \equiv g^k + 2$ (mód p) es imposible para cualquier k.**

Suponiendo que fuera cierto tendríamos $g^{k+1}(g-1) \equiv g^k(g-1)$ (mód p) y de ahí, $g^{k+1} \equiv g^k$ (mód p), lo cual es imposible.

20. *a*) **Demostrar que si m es un número con raíces primitivas, entonces el producto de enteros menores o iguales que m y primos relativos con m es congruente con -1 (mód m).**

b) **Demostrar que el resultado de *a*) no es siempre cierto si m no tiene raíces primitivas**.

a) Si m tiene una raíz primitiva g, $g, g^2, \ldots, g^{\phi(m)}$ son una permutación de los $\phi(m)$ enteros positivos $r_1, r_2, \ldots, r_{\phi(m)}$ menores que m y primos relativos con m y son raíces del polinomio $x^{\phi(m)} - 1$ (mód p). Entonces,

$$x^{\phi(m)} - 1 \text{ (mód } p) = (x - r_1)(x - r_2) \cdots (x - r_{\phi(m)}) \text{ (mód } p).$$

Sustituyendo por $x = 0$, y teniendo en cuenta que $\phi(m)$ es par, obtenemos $r_1 r_2 \cdots r_{\phi(m)} \equiv -1$ (mód p).

b) Para $m = 8$, tenemos $1^2 \equiv 3^2 \equiv 5^2 \equiv 7^2 \equiv 1$ (mód 8), por lo que ninguno de los órdenes de 1, 3, 5, y 7 es $4 = \phi(8)$ y 8 no tiene raíces primitivas. En este caso tenemos $1 \cdot 3 \cdot 5 \cdot 7 = 1$ (mód 8).

11. Congruencias cuadráticas

1. **¿Cuáles de las siguientes congruencias tiene solución?**

$$x^2 \equiv 7 \text{ (mód } 53) \qquad x^2 \equiv 14 \text{ (mód } 31)$$
$$x^2 \equiv 53 \text{ (mód } 7) \qquad x^2 \equiv 25 \text{ (mód } 997)$$

a) Según el criterio de Euler, la congruencia $x^2 \equiv 7$ (mód 53) tiene alguna solución si y solo si $7^{26} \equiv 1$ (mód 53). Hallamos $7^2 = 49 = -4$ (mód 53), $7^4 = 16$ (mód 53), $7^8 = 256 = -9$ (mód 53), $7^{12} = -144 = 15$ (mód 53), $7^{13} = 105 = -1$ (mód 53), $7^{26} = 1$ (mód 53).

b) $x^2 \equiv 53$ (mód 7) $\Leftrightarrow x^2 \equiv 4$ (mód 7), que tiene una solución evidente: $x = 2$.

Observación: Como $53 \equiv 1$ (mód 3), el teorema de reciprocidad cuadrática nos dice esta congruencia tiene solución si y solo si la tiene la congruencia del apartado anterior. Usando el símbolo de Legendre, podíamos haber respondido a los dos apartados con los cálculos:

$$\left(\frac{7}{53}\right) = \left(\frac{53}{7}\right) = \left(\frac{4}{7}\right) = \left(\frac{2^2}{7}\right) = 1.$$

c) Según el criterio de Euler, la congruencia $x^2 \equiv 14$ (mód 31) tendrá una solución si y solo si $14^{15} \equiv 1$ (mód 31). Como $2^5 = 32 \equiv 1$ (mód 31), entonces $2^{15} \equiv 1$ (mód 31). Ahora calculamos unas pocas potencias de 7 (mód 31) : $7^2 = 49 \equiv 18$, $7^4 \equiv 324 \equiv 14$, $7^8 \equiv 196 \equiv 10$, $7^{16} \equiv 100 \equiv 7 \Rightarrow 7^{15} \equiv 1$ (mód 31). Por tanto, la congruencia tiene solución.

Usando el símbolo de Legendre llegamos al mismo resultado de una forma más rápida y sencilla:

$$\left(\frac{14}{31}\right) = \left(\frac{2}{31}\right)\left(\frac{7}{31}\right) = 1 \cdot \left[-\left(\frac{31}{7}\right)\right] =$$
$$= -\left(\frac{3}{7}\right) = \left(\frac{7}{3}\right) = \left(\frac{1}{3}\right) = 1.$$

d) Observando que $25 = 5^2$ es un cuadrado, $x \equiv 5$ es una solución inmediata de la congruencia $x^2 \equiv 25$ (mód 997).

2. **¿Cuáles de las siguientes congruencias tiene solución?**

$$x^2 \equiv 8 \text{ (mód 53)} \qquad x^2 \equiv 15 \text{ (mód 31)}$$
$$x^2 \equiv 54 \text{ (mód 7)} \qquad x^2 \equiv 625 \text{ (mód 9973)}$$

a) Hallemos 8^{26} (mód 53) y usemos el criterio de Euler. Tenemos $8^2 = 64 \equiv 11$ (mód 53), $8^4 \equiv 121 \equiv 15$ (mód 53), $8^6 = 165 \equiv 6$ (mód 53), $8^{12} \equiv 36$ (mód 53), $8^{13} \equiv 288 \equiv 23$ (mód 53), $8^{26} \equiv 529 \equiv -1$ (mód 53). Según el criterio de Euler, esta congruencia no tiene solución. El mismo resultado se obtiene usando el símbolo de Legendre:

$$\left(\frac{2}{53}\right) = -1 \Rightarrow \left(\frac{8}{53}\right) = \left(\frac{2^3}{53}\right) = \left(\frac{2}{53}\right)^3 = (-1)^3 = -1.$$

b) La congruencia $x^2 \equiv 54$ (mód 7) no tiene ninguna solución, como podemos ver fácilmente usando el símbolo de Legendre:

$$\left(\frac{54}{7}\right) = \left(\frac{5}{7}\right) = \left(\frac{7}{5}\right) = \left(\frac{2}{5}\right) = -1.$$

c) Lo mismo le ocurre a la congruencia $x^2 \equiv 15$ (mód 31):

$$\left(\frac{15}{31}\right) = \left(\frac{3}{31}\right) \cdot \left(\frac{5}{31}\right) = -\left(\frac{31}{3}\right) \cdot \left(\frac{31}{5}\right) = -\left(\frac{1}{3}\right) \cdot \left(\frac{1}{5}\right) = -1.$$

d) Observando que $625 = 25^2$ es un cuadrado, $x \equiv 25$ es una solución inmediata de la congruencia $x^2 \equiv 625$ (mód 9973).

3. **Encontrar soluciones de las congruencias del Problema 1 que las tengan**.

Para resolver $x^2 \equiv 7$ (mód 53), tenemos en cuenta que $7 \equiv 60 \equiv 113 \equiv 166 \equiv 219 \equiv 272 \equiv 325 \equiv 378 \equiv 431 \equiv 484 = 22^2$ (mód 53) Las soluciones son $x = 22$ y $x = 31$ (mód 53).

De $x^2 \equiv 53$ (mód 7), que es equivalente a $x^2 \equiv 4$ (mód 7), la soluciones son evidentemente $x = 2$ y $x = 5$ (mód 7).

Para resolver $x^2 \equiv 14$ (mód 31), tenemos en cuenta que $14 \equiv 45 \equiv 76 \equiv 107 \equiv 138 \equiv 169 = 13^2$ (mód 31). Las soluciones son $x = 13$ y $x = 18$ (mód 31).

Por último la soluciones de $x^2 \equiv 25$ (mód 997) son $x = 5$ y $x = 992$ (mód 997).

4. **Encontrar soluciones de las congruencias del Problema 2 que las tengan**.

   La única congruencia con solución es $x^2 \equiv 625 \pmod{9973}$, y sus soluciones son $x = 25$ y $x = 9948 \pmod{9973}$.

5. **Calcular** $(33/71)$**,** $(34/71)$**,** $(35/71)$**,** $(36/71)$.

   a) $$\begin{aligned}(33/71) =&(3/71)(11/71) = -(71/3)\ \cdot[-(71/11)] = \\ =&(2/3)\cdot(5/11) = (-1)\cdot(11/5) = (-1)\cdot 1 = -1.\end{aligned}$$

   b) $$\begin{aligned}(34/71) =&(2/71)(17/71) = 1\ \cdot(71/17) = \\ =&(3/17) = (17/3) = (2/3) = -1.\end{aligned}$$

   c) $$\begin{aligned}(35/71) =&(5/71)(7/71) = (71/5)\cdot[-(71/7)] = \\ =&-\,(1/5)\cdot(1/7) = -1\cdot 1 = -1.\end{aligned}$$

   d) $(36/71) = (6^2/71) = 1.$

6. **Calcular** $(33/73)$**,** $(34/73)$**,** $(35/73)$**,** $(36/73)$.

   a) $$\begin{aligned}(33/73) =&(3/73)(11/73) = (73/3)\cdot(73/11) = \\ =&(1/3)\cdot(7/11) = 1\cdot[-(11/7)] = -(4/7) = -1.\end{aligned}$$

   b) $$\begin{aligned}(34/73) =&(2/73)(17/73) = 1\ \cdot(73/17) = \\ =&(5/17) = (17/5) = (2/5) = -1.\end{aligned}$$

   c) $$\begin{aligned}(35/73) =&(5/73)(7/73) = (73/5)\cdot(73/7) = (3/5)\cdot(3/7) = \\ =&(5/3)\cdot[-(7/3)] = -(2/3)(4/3) = 1.\end{aligned}$$

   d) $(36/73) = (6^2/73) = 1.$

7. **Resolver** $2x^2 + 3x + 1 = 0$ **(mód** 7**) y** $2x^2 + 3x + 1 = 0$ **(mód** 101**)**.

   a) Multiplicando $2x^2+3x+1 \equiv 0 \pmod 7$ por 4, resulta, $x^2+5x+4 \equiv 0 \pmod 7$, que es equivalente a $x^2 + 12x + 4 \equiv 0 \pmod 7$. Ahora completamos cuadrados: $x^2+12x+36 \equiv 32 \pmod 7 \Rightarrow (x+6)^2 \equiv 4 \mod 4 \Rightarrow x + 6 \equiv \pm 2$. Hay dos soluciones $x \equiv -4$ y $x \equiv -8$, o $x \equiv 3$ y $x \equiv 6$.

b) Multiplicamos $2x^2 + 3x + 1 = 0$ (mód 101) por 51 y obtenemos la congruencia $x^2 + 52x + 51 \equiv 0$ (mód 101). Ahora completamos cuadrados: $x^2 + 52x + 676 \equiv 625$ (mód 101) $\Rightarrow (x + 26)^2 \equiv 25^2$ (mód 101) $\Rightarrow x+26 \equiv \pm 25$ (mód 101). Las soluciones son $x = -1$ y $x = -51$ (mód 101), es decir $x = 50$ y $x = 100$ (mód 101).

8. **Resolver** $3x^2 + x + 8 \equiv 0$ **(mód** 11**) y** $3x^2 + x + 52 \equiv 0$ **(mód** 11**).**

a) Multiplicamos $3x^2 + x + 8 \equiv 0$ (mód 11) por 4 para obtener $x^2 + 4x + 10 \equiv 0$ (mód 11) y ahora completamos cuadrados: $x^2 + 4x + 4 \equiv 5$ (mód 11) ó $(x + 2)^2 \equiv 5$ (mód 11) $\Leftrightarrow (x + 2)^2 \equiv 16$ (mód 11) $\Leftrightarrow x + 2 \equiv \pm 4$ (mód 11). Las soluciones son $x \equiv 2$ y $x \equiv 5$ (mód 11).

b) $3x^2 + x + 52 \equiv 0$ (mód 11) y $3x^2 + x + 52 \equiv 0$ (mód 11) son congruencias equivalentes, por lo que $3x^2 + x + 52 \equiv 0$ (mód 11) también tiene por soluciones $x \equiv 2$ y $x \equiv 5$ (mód 11).

9. **Calcular** $(1234/4567)$ **y** $(4321/4567)$**.**

$$\begin{aligned}(1234/4567) =&(2/4567) \cdot (617/4567) = 1 \cdot (4567/617) = (248/617) = \\ =&(8/617) \cdot (31/617) = 1^3 \cdot (617/31) = (28/31) = \\ =&(7/31) = -(31/7) = -(3/7) = (7/3) = (1/3) = 1.\\ (4321/4567) =&(29/4567) \cdot (149/4567) = (4567/29) \cdot (4567/149) = \\ =&(14/29) \cdot (97/149) = (2/29) \cdot (7/29) \cdot (149/97) = \\ =&-1 \cdot (29/7) \cdot (52/97) = -1(1/7) \cdot (4/97) \cdot (13/97) = \\ =&-(13/97) = -(97/13) = -(6/13) = -(2/13)(3/13) = \\ =&(3/13) = (13/3) = (1/3) = 1.\end{aligned}$$

10. **Calcular** $(1356/2467)$ **y** $(6531/2467)$**.**

$$\begin{aligned}(1356/2467) =&(3/2467) \cdot (7/2467) \cdot (311/2467) = \\ =&1 \cdot [-(2467/3)] \cdot (2467/113) = \\ =&-(1/3) \cdot (94/113) = -(2/113) \cdot (47/113) = \\ =&-(113/47) = -(19/47) = +(47/19) = (9/19) = 1.\end{aligned}$$

$$\begin{aligned}(6531/2467) =&(3/2467)\cdot(7/2467)\cdot(311/2467)=\\ &=[-(2467/3)]\cdot[-(2467/7)]\cdot[-(2467/311)]=\\ &=-(1/3)\cdot(3/7)\cdot(290/311)=\\ &=+(7/3)\cdot(2/311)\cdot(5/311)\cdot(29/311)=\\ &=1\cdot 1\cdot(311/5)\cdot(311/29)=(1/5)\cdot(21/29)=\\ &=(3/29)\cdot(7/29)=(29/3)\cdot(29/7)=(2/3)\cdot(1/7)=-1.\end{aligned}$$

11. **Demostrar que si $p=q+4a$ (p y q son primos impares), entonces $(p/q)=(a/q)$.**

    Si $(p/q)=1$, la congruencia $x^2\equiv p\ (\text{mód } q)$ tiene una solución x_0. Podemos considerar que x_0 es par, pues en caso contrario, podemos tomar $p-x_0$, que también es solución. Llamando $x_1=\frac{x_0}{2}$, tenemos que $x_1^2=\frac{x_0^2}{4}\equiv\frac{p}{4}\equiv\frac{p-q}{4}=a\ (\text{mód } q)$. Es decir, también es $(a/q)=1$.

    Partiendo ahora de $(a,q)=1$, $x^2\equiv a\ (\text{mód } q)$ tiene una solución x_1. Llamando $x_0=2x_1$, $x_0^2=4x_1^2\equiv 4a\equiv q+4a=p\ (\text{mód } q)$. Conclusión: $(p/q)=1$.

12. **Demostrar que si $p=12k+1$ para algún k, entonces $(3/p)=1$.**

    Usamos el símbolo de Legendre: $(3/p)=(p/3)=(1/3)=1$.

13. **Demostrar que el teorema 6 puede expresarse también diciendo que $(2/p)=(-1)^{\frac{p^2-1}{8}}$ para cualquier primo impar p.**

    El teorema 6 dice que $(2/p)=1$ si $p=1,7\ (\text{mód } 8)$ y que $(2/p)=-1$ si $p=3,5\ (\text{mód } 8)$. Si $p=1,7\ (\text{mód } 8)$, entonces $p=\pm 1\ (\text{mód } 8)$, por lo que $p=8k\pm 1$ para algún k y $p^2-1=64k^2\pm 16k\Rightarrow\frac{p^2-1}{8}=8k^2\pm 2k$ es par. Si $p=3,5\ (\text{mód } 8)$, $p=\pm 3\ (\text{mód } 8$, por lo que $p=8k\pm 3$ para algún k. Entonces $p^2-1=64k^2\pm 48k+8$ y $\frac{p^2-1}{8}=8k^2\pm 6k+1$ es impar.

14. **Demostrar que el teorema de reciprocidad cuadrática también puede escribirse**

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right)=(-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}},$$

    siendo p y q primos impares.

Basta tener en cuenta que cuando p es un primo impar, $\frac{p-1}{2}$ es par si $p \equiv 1$ (mód 4) e impar si $p \equiv 3$ (mód 4).

Si $p, q \equiv 3$ (mód 4) los símbolos (p/q) y (q/p) son opuestos, por lo que su producto es -1. Como $\frac{p-1}{2}$ y $\frac{q-1}{2}$ son impares, también lo es el producto de ambos, así que $(-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}} = -1$.

Si $p \equiv 1$ (mód 4) o $q \equiv 1$ (mód 4), alguno de los números $\frac{p-1}{2}$ o $\frac{q-1}{2}$ será par, así que también lo será el producto de ambos y tendremos $(-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}} = 1$, que coincide con el valor de $(p/q)(q/p)$, ya que en este caso los símbolos son iguales.

15. **El estudiante A dice: "He comprobado todos los números hasta el 100 y todavía no he encontrado ningún n tal que n^2+1 sea divisible por 7. Ahora estoy cansado, así que ya encontraré uno mañana". El estudiante B, después de unos pocos segundos pensando, dice: "No, no lo encontrarás". ¿Cómo lo supo B tan rápidamente?**

Como $(-1/7) = -1$, -1 no es un residuo cuadrático módulo 7 y la congruencia $x^2 \equiv -1$ (mód 7) no tiene solución.

16. **Demostrar que si a es un residuo cuadrático (mód p) y $ab = 1$ (mód p), entonces b es un residuo cuadrático (mód p).**

Usando el símbolo de Legendre, si a es un residuo cuadrático (mód p), tendremos $(a/p) = 1$. Entonces

$$\left(\frac{b}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right) = \left(\frac{ab}{p}\right) = \left(\frac{1}{p}\right) = 1,$$

por lo que b también es un residuo cuadrático (mód p).

17. **¿Tiene $x^2 = 211$ (mód 159) alguna solución? Observar que 159 no es primo.**

Como, $153 = 3 \cdot 53$, es equivalente al sistema

$$\left\{\begin{array}{l} x^2 = 211 \text{ (mód 3)} \\ x^2 = 211 \text{ (mód 53)} \end{array}\right. , \left\{\begin{array}{l} x^2 = 1 \text{ (mód 3)} \\ x^2 = 52 \text{ (mód 53)} \end{array}\right. , \left\{\begin{array}{l} x = 2 \text{ (mód 3)} \\ x^2 = 52 \text{ (mód 53)} \end{array}\right.$$

Como $(1/3) = 1 = (-1/53)$, las dos ecuaciones tienen solución por separado. Teniendo en cuenta que $52 \equiv 105 \equiv 158 \equiv 211 \equiv 264 \equiv$

$317 \equiv 370 \equiv 423 \equiv 476 \equiv 529 = 23^2$ (mód 53), $x = 23$ es solución de la segunda ecuación, resultando también solución de la primera. Otras soluciones son 76, 83 y 136.

18. **Demostrar que si $p \equiv 3$ (mód 8) y $\frac{p-1}{2}$ es primo, entonces $\frac{p-1}{2}$ es un residuo cuadrático (mód p).**

    Sea $q = \frac{p-1}{2}$. Como $p = 8k + 3$ para algún k, q es de ka forma $4k + 1$. Además, es $p = 2q + 1$. Por todo ello, $(q/p) = (p/q) = (1/q) = 1$, así que q es un residuo cuadrático (mód p).

19. **Generalizar el problema 16 con condiciones sobre r que garanticen que si a es un resto cuadrático (mód p) y $ab \equiv r$ (mód p), entonces b es un resto cuadrático (mód p).**

    Supongamos que r es un residuo cuadrático (mód p), en cuyo caso tendremos $(r/p) = 1$. Si a es un residuo cuadrático (mód p) y $ab \equiv r$ (mód p),

    $$\left(\frac{b}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right) = \left(\frac{ab}{p}\right) = \left(\frac{r}{p}\right) = 1,$$

    por lo que b también es un residuo cuadrático (mód p). La condición $(r/p) = 1$ es entonces suficiente. Evidentemente, también es necesaria pues si a y b son residuos cuadráticos

20. **Supongamos que $p = q + 4a$, donde p y q son primos impares. Demostrar que $(a/p) = (a/q)$.**

12. Reciprocidad cuadrática

1. **Adaptar el método usado en el texto para evaluar** $(2/p)$ **para evaluar** $(3/p)$.

   Hay que contar cuántos números a hay tales que $\frac{p-1}{2} < 3a < p$, o bien, tales que, $\frac{p-1}{6} < a < \frac{p}{3}$ (en los casos en que $3a > p$, nunca es $3a > p + \frac{p-1}{2}$, así que $3a$ no produce un resto mayor que $\frac{p-1}{2}$).

   Sea entonces g el número de números a que cumplen $\frac{p-1}{6} < a < \frac{p}{3}$, y tendremos entonces que $(3/p) = (-1)^g$.

   Sea $p = 12k + 1$. Entonces $\frac{p-1}{6} = 2k$ y $\frac{p}{3} = 4k + \frac{1}{3}$. Debe ser $2k < a < 4k + \frac{1}{3}$, es decir, $2k+1 \leq a \leq 4k$. En este caso $g = 4k-(2k+1)+1 = 2k$ y $(3/p) = 1$.

   Sea $p = 12k + 5$. Entonces $\frac{p-1}{6} = 2k + \frac{2}{3}$ y $\frac{p}{3} = 4k + \frac{5}{3}$. Debe ser $2k + \frac{2}{3} < a < 4k + \frac{5}{3}$, es decir, $2k + 1 \leq a \leq 4k + 1$. En este caso $g = (4k + 1) - (2k + 1) + 1 = 2k + 1$ y $(3/p) = -1$.

   Sea $p = 12k + 7$. Entonces $\frac{p-1}{6} = 2k + 1$ y $\frac{p}{3} = 4k + \frac{7}{3}$. Debe ser $2k + 1 < a < 4k + \frac{7}{3}$, es decir, $2k + 1 \leq a \leq 4k + 2$. En este caso $g = (4k + 2) - (2k + 2) + 1 = 2k + 1$ y $(3/p) = -1$.

   Sea $p = 12k + 11$. Entonces $\frac{p-1}{6} = 2k + \frac{5}{3}$ y $\frac{p}{3} = 4k + \frac{11}{3}$. Debe ser $2k + \frac{5}{3} < a < 4k + \frac{11}{3}$, es decir, $2k + 2 \leq a \leq 4k + 3$. En este caso $g = (4k + 3) - (2k + 2) + 1 = 2k + 2$ y $(3/p) = 1$.

   Entonces, podemos expresar:

$$\left(\frac{3}{p}\right) = \begin{cases} 1 \text{ si } p \equiv \pm 1 \text{ (mód 12)} \\ -1 \text{ si } p \equiv \pm 5 \text{ (mód 12)} \end{cases}.$$

2. **Demostrar que 3 es un no-residuo cuadrático de todos los primos de la forma** $4^n + 1$.

   Para cualquier n, es $4^n + 1 \equiv 1$ (mód 4) y $4^n \equiv 1$ (mód 3). Por tanto,

$$\left(\frac{3}{4^n + 1}\right) = \left(\frac{4^n + 1}{3}\right) = \left(\frac{2}{3}\right) = -1.$$

3. **Demostrar que 3 es un no-residuo cuadrático de todos los primos de Mersenne mayores que** 3.

Si $p > 2$, $2^p - 1 = 4 \cdot 2^{p-2} - 1 = 4 \cdot (2^{p-2} - 1) + 3 \equiv 3 \pmod 4$ y $2^p \equiv 2 \pmod 3$. Por tanto,

$$\left(\frac{3}{2^p - 1}\right) = -\left(\frac{2^p - 1}{3}\right) = -\left(\frac{1}{3}\right) = -1.$$

4. *a*) **Demostrar que si $p \equiv 7 \pmod 8$, entonces $p|(2^{(p-1)/2} - 1)$.**

   b) **Encontrar un factor de $2^{83} - 1$.**

   a) $p|(2^{(p-1)/2} - 1) \Leftrightarrow 2^{(p-1)/2} \equiv 1 \pmod p \Leftrightarrow (2/p) = 1$. Siempre que $p \equiv 7 \pmod 8$, tenemos que $(2/p) = 1$, así que entonces $p|(2^{(p-1)/2} - 1)$.

   b) Haciendo que $\frac{p-1}{2} = 83$, obtenemos $p = 167$, así que $p = 167$ es un factor de $2^{83} - 1$.

5. *a*) **Si $p =$ y $q = 10p + 3$ son primos impares, demostrar que $(p/q) = (3/p)$.**

   b) **Si $p =$ y $q = 10p + 1$ son primos impares, demostrar que $(p/q) = (-1/p)$.**

   a) Si $p \equiv 1 \pmod 4$, entonces $(p/q) = (q/p)$. Si $p \equiv 3 \pmod 4$, $10p + 3 \equiv 33 \equiv 1 \pmod 4$ y también es $(p/q) = (q/p)$. Por tanto, tenemos que $(p/q) = (q/p) = (3/p)$.

   b) Si $p \equiv 1 \pmod 4$, $(p/q) = (q/p) = (1/p) = 1 = (-1/p)$.
   Si $p \equiv 3 \pmod 4$, $(p/q) = -(q/p) = -(1/p) = -1 = (-1/p)$.

6. *a*) **¿Qué primos pueden dividir a $n^2 + 1$ para algún n?**

   b) **¿Qué primos pueden dividir a $n^2 + n$ para algún n?**

   c) **¿Qué primos pueden dividir a $n^2 + 2n + 2$ para algún n?**

   a) Aquellos para los que $x^2 \equiv -1 \pmod p$ tiene solución es decir, aquellos para los que $(-1/p) = 1$. Entonces son los $p \equiv 3 \pmod 4$.

   b) Es evidente que cualquier primo p divide a $n^2 + n$ siendo $n = p$, así que la respuesta en este caso es "Todos los primos".

   c) $n^2+2n+2 \equiv 0 \pmod p \Leftrightarrow n^2+2n+1 = -1 \pmod p \Leftrightarrow (n+1)^2 \equiv -1 \pmod p$. También son los $p \equiv 3 \pmod 4$.

7. *a*) **Demostrar que si $p \equiv 3$ (mód 4) y a es un residuo cuadrático (mód p), entonces $p - a$ es un no-residuo cuadrático (mód p).**

   b) **¿Qué ocurre si $p \equiv 1$ (mód 4)?**

   a)
   $$\left(\frac{p-a}{p}\right) = \left(\frac{-a}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{-1}{p}\right) = -\left(\frac{a}{p}\right) = -1$$

   b)
   $$\left(\frac{p-a}{p}\right) = \left(\frac{-a}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{-1}{p}\right) = 1 \cdot 1 = -1.$$

8. **Si $p > 3$, demostrar que p divide a la suma de sus residuos cuadráticos que también son restos**.

   Los residuos cuadráticos $a_1, \ldots, a_r$, con $r = \frac{p-1}{2}$ que son restos pueden considerarse cuadrados de los números $1, \ldots, r$. Usando la fórmula
   $$1^2 + 2^2 + \cdots + n^2 = \frac{n^3}{3} + \frac{n^2}{2} + \frac{n}{6} = \frac{n(n+1)(2n+1)}{6},$$
   obtenemos
   $$a_1 + \cdots + a_r = \frac{r(r+1)(2r+1)}{6} = \frac{(p-1)(p+1)p}{24} \equiv 0 \text{ (mód } p).$$

9. **Si p es un primo impar, evaluar**
   $$(1 \cdot 2/p) + (2 \cdot 3/p) + \cdots + ((p-2) \cdot (p-1)/p).$$

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
1	1	-1	1	-1	-1	-1	1	1	-1	-1	-1	1	-1	1	1
1	-1	-1	-1	1	1	-1	1	-1	1	1	-1	-1	-1	1	

10. **Demostrar que si $p \equiv 1$ (mód 4), entonces $x^2 \equiv -1$ (mód p) tiene una solución dada por el resto (mód p) de $((p-1)/2)!$.**