El último teorema de Fermat y los números de Mersenne

por

Laureano Pérez-Cacho

(Trabajo premiado por la Academia en el Concurso Ordinario de 1946)

RESUMEN

Hacemos constar que el contenido de las páginas siguientes se ha obtenido basándose exclusivamente:

1.º En el trabajo *sobre el último teorema de Fermat*, L. Pérez Cacho, «Revista Hispano Americana», Madrid, 1928.

2.º En el teorema fundamental de Euler «Todos los divisores de los números de Mersenne (n primo) son de la forma $2\,\mathrm{K}\,n + 1$».

3.º En la proposicion «Todos los divisores de los números de Mersenne son de la forma $8\,\mathrm{K} \pm 1$ (K natural $n \geqq 3$)».

4.º En la propiedad «Todos los divisores primos impares de la expresión $x^2 - 5$ son 5 y los números primos de la forma $10\,\mathrm{K} \pm 1$».

Tomando como punto de partida el enunciado del teorema de Fermat y teniendo en cuenta nuestro trabajo (1.º) hemos expuesto un método basado exclusivamente en la teoría de las congruencias.

Exponemos a continucción un segundo procedimiento que nos conduce a la irreducibilidad de ecuaciones; este es a nuestro juicio el más interesante.

He aquí algunos de los resultados obtenidos:

a) El teorema de Fermat es equivalente al siguiente:

«Demostrar que la ecuación cuadrática

$$z^2 - a^n z + a = 0 \qquad n > 1$$

es irreducible en K (1) siendo a un elemento del cuerpo K (1).»

b) «Si el teorema de Fermat es cierto, las tangentes a la parábola $y^2 = 4x$ en sus puntos racionales cortan a las parábolas $y = x^n$ $(n \geqq 2)$ en puntos irracionales.»

c) Se ha demostrado la congruencia fundamental

$$A + B \equiv 0 \pmod{n^2}$$

siendo $2^n - 1 = AB$ y de esta propiedad se ha deducido la congruencia

$$A + B \equiv 0 \pmod{16}$$

Se ha obtenido la condición necesaria y suficiente para que $2^n - 1$ sea compuesto.

Finalmente se ha estudiado un caso particular, que nos ha conducido al estudio de las soluciones enteras de la ecuación

$$2^{n+4} - 7 = h^2$$

por el cual podrá juzgar el lector la dificultad del problema general.

1. El teorema de Fermat es «Si n es un entero positivo > 2, la ecuación

$$x^n + y^n = z^n \qquad [1]$$

no puede verificarse para valores enteros de las incógnitas $x, y, z,$ al menos que una de ellas sea nula».

Para $n = 1$ y $n = 2$ la ecuación [1] admite, como es bien sabido, infinitas soluciones.

El teorema ha sido demostrado para $n = 4$ por Leibnitz en 1678 y posteriormente por Euler.

Bastará demostrarlo para n impar y mayor que 1.

2. *Primer metodo.*—Supondremos, como de ordinario, que en la ecuación [1] es n primo mayor que 2, que x, y, z son enteros, positivos, primos dos a dos y además con n.

Observemos, en primer lugar, que la ecuación [1] supuesta satisfecha, puede escribirse

$$(z - y)(z^{n-1} + yz^{n-2} + \ldots\ldots + y^{n-1}) = x^n$$

y que si se demuestra que los dos factores del primer miembro

$$z - y, \qquad z^{n-1} + yz^{n-2} + \ldots\ldots + y^{n-1}$$

son primos entre sí, tendrán que ser dos potencias n-ésimas perfectas

$$z - y = a^n \qquad z^{n-1} + y\,z^{n-2} + \ldots\ldots + y^{n-1} = b^n$$

siendo $x = a\,b$ y $m\,c\,d\,(a, b) = 1$ no excluyendo el caso $a = 1$. Pero

$$z - y, \qquad z^{n-1} + y\,z^{n-2} + \ldots\ldots + y^{n-1}$$

tienen que ser primos entre sí porque si tuviesen un factor primo común $d > 1$ es decir, si fuese

$$z - y = m\,d \qquad z^{n-1} + y\,z^{n-2} + \ldots\ldots + y^{n-1} = m_1\,d$$

se tendría

$$(y + m\,d)^{n-1} + (y + m\,d)^{n-2}\,y + \ldots\ldots + y^{n-1} = m_1\,d$$

de donde

$$n\,y^{n-1} + m_2\,d = m_1\,d \qquad \text{ó sea} \qquad n\,y^{n-1} = m_3\,d.$$

Ahora bien, por hipótesis n e y son primos entre sí y, por tanto, d tiene que dividir a n o a y. A y no puede dividirlo, pues, por ser $z = y + m\,d$ dividiría a z, no siendo entonces z e y primos entre sí. Tampoco puede dividir a n puesto que por la congruencia de Fermat se deduce

$$\left.\begin{aligned} x^{n-1} &\equiv 1 \\ y^{n-1} &\equiv 1 \\ z^{n-1} &\equiv 1 \end{aligned}\right\} \pmod{n} \qquad \text{es decir} \qquad \left.\begin{aligned} x^n &\equiv x \\ y^n &\equiv y \\ z^n &\equiv z \end{aligned}\right\} \pmod{n}$$

y siendo

$$x^n + y^n = z^n$$

sería

$$x + y \equiv z \pmod{n}$$

o lo que es lo mismo

$$z - y \equiv x \pmod{n}$$

y por ser

$$z - y = m\,d$$

resultaría

$$z - y \equiv 0 \pmod{n}$$

y por lo tanto

$$x \equiv 0 \pmod{n}$$

lo cual es imposible por haberse supuesto x primo con n.

Queda así establecido que se tiene

$$z - y = a^n, \qquad z^{n-1} + y z^{n-2} + \ldots\ldots + y^{n-1} = b^n$$

siendo $x = a\,b$ y $m\,c\,d\,(a, b) = 1$.

Sentado ésto, de la congruencia

$$z - y \equiv x \pmod{n}$$

resulta

$$a^n \equiv a\,b \pmod{n}$$

y por ser a primo con n (puesto que a divide a x, y x es primo con n por hipótesis) se tiene

$$b \equiv a^{n-1} \pmod{n}$$

o sea

$$b \equiv 1 \pmod{n} \qquad [\alpha]$$

Análogamente se establece que

$$\left.\begin{array}{l} b_1 \equiv 1 \\ b_2 \equiv 1 \end{array}\right\} \pmod{n} \qquad [\beta]$$

si se supone, respectivamente

$$\begin{array}{ll} y = a_1\,b_1 & m\,c\,d\,(a_1\,, b_1) = 1 \\ z = a_2\,b_2 & m\,c\,d\,(a_2\,, b_2) = 1 \end{array}$$

correspondientes a las hipótesis

$$\begin{array}{ll} z - x = a_1^n\,, & z^{n-1} + x\,z^{n-2} + \ldots\ldots + x^{n-1} = b_1^n \\ x + y = a_2^n\,, & x^{n-1} - y\,x^{n-2} + \ldots\ldots + y^{n-1} = b_2^n \end{array}$$

3. Vamos a demostrar que se verifica

$$x + y \equiv z \pmod{n^2}.$$

En efecto: La ecuación [1] teniendo en cuenta que es $x = a\,b \quad y = a_1\,b_1$ $z = a_2\,b_2$ se convierte en la

$$a^n b^n + a_1^n b_1^n = a_2^n b_2^n$$

o sea

$$(z - y)\,b^n + (z - x)\,b_1^n = (x + y)\,b_2^n \qquad [8]$$

y teniendo en cuenta las congruencias [α] y [β] se tiene

$$b^n \equiv b_1^n \equiv b_2^n \equiv 1 \qquad (\text{mod } n^2)$$

y de éstas y de [8] se deduce

$$(z - x) + (z - y) \equiv (x + y)\,(\text{mod } n^2)$$

de donde

$$2\,z \equiv 2\,x + 2\,y \qquad (\text{mod } n^2).$$

y por ser $m\,c\,d\,(2, n) = 1$ se obtiene

$$x + y \equiv z \qquad (\text{mod } n^2)$$

como se quería demostrar.

4. De los resultados obtenidos se deduce un procedimiento para demostrar el teorema de Fermat; es el siguiente: «Supongamos se verifica

$$x + y \equiv z \qquad (\text{mod } n^k)$$

para cualquier valor de $K > 2$.

Si con esta hipótesis *se pudieran demostrar* las congruencias

$$b \equiv b_1 \equiv b_2 \equiv 1 \qquad (\text{mod } n^k)$$

por un razonamiento similar al del párrafo anterior quedaría demostrado

$$x + y \equiv z \qquad (\text{mod } n^{k+1}) \quad »$$

En efecto: Por ser

$$b \equiv b_1 \equiv b_2 \equiv 1 \qquad (\text{mod } n^k)$$

será

$$b^n \equiv b_1^n \equiv b_2^n \equiv 1 \qquad (\text{mod } n^{k+1})$$

y de éstas y de la igualdad [8] del párrafo anterior se tiene

$$(z - x) + (z - y) \equiv (x + y) \qquad (\text{mod } n^{k+1})$$

y de aquí simplificando

$$x + y \equiv z \qquad (\text{mod } n^{k+1})$$

y como esta congruencia es cierta para $K = 0$ y $K = 1$ según hemos demostrado, sería también cierta para todo valor de K; es decir, $x + y - z$ sería mayor que cualquier número por grande que fuera, lo cual es imposible, pues x, y, z son números finitos; y el teorema de Fermat quedaría demostrado en el supuesto de que ninguna de las incógnitas x, y, z, sea divisibles por n.

5. *Segundo método.*—Suponemos la ecuación de Fermat puesta en la forma

$$a^{2n-1} + b^{2n-1} = c^{2n-1} \qquad \text{[II]}$$

donde el exponente es indiferente sea o no un número primo, y a, b, c enteros no nulos.

El teorema de Fermat puede enunciarse del siguiente modo: «Demostrar que la ecuación [II] para $n > 1$ no puede verificarse para valores enteros de las incógnitas».

6. *Teorema fundamental.*—«La condición necesaria y suficiente para que la ecuación [II] admita una solución en números enteros, es que la ecuación

$$(x\,y)^n = x + y \qquad \text{[III]}$$

admita una solución (x, y) racional.»

En efecto: Sea (a, b, c) una solución de la ecuación [II] siendo a, b, c enteros ordinarios; hagamos

$$x = \frac{c\,a^{n-1}}{b^n}, \qquad y = \frac{c\,b^{n-1}}{a^n}$$

siendo por tanto x, y números racionales.

Sustituyendo estos valores en la [III] se obtiene

$$\left(\frac{c\,a^{n-1}}{b^n} \cdot \frac{c\,b^{n-1}}{a^n}\right)^n = \frac{c\,a^{n-1}}{b^n} + \frac{c\,b^{n-1}}{a^n}$$

y simplificando

$$\left(\frac{c^2}{a\,b}\right)^n = \frac{c\,(a^{2n-1} + b^{2n-1})}{(a\,b)^n}$$

igualdad cierta por ser por hipótesis

$$a^{2n-1} + b^{2n-1} = c^{2n-1}$$

Recíprocamente: Sea $x = \frac{\alpha}{\delta}$ $y = \frac{\beta}{\delta}$ una solución racional de la ecuación [III]; siempre podemos suponer $m\,c\,d\,(\alpha, \beta, \delta,) = 1$.

Sustituyendo x y por sus valores en la [III] se tendrá

$$\left(\frac{\alpha}{\delta} \cdot \frac{\beta}{\delta}\right)^n = \frac{\alpha}{\delta} + \frac{\beta}{\delta}$$

simplificando

$$(\alpha\,\beta)^n = (\alpha + \beta)\,\delta^{2n-1}$$

Sea $m\,c\,d\,(\alpha, \beta) = d$ siendo $\alpha = d\,\alpha_1$ $\beta = d\,\beta_1$ y, por tanto, $m\,c\,d\,(\alpha_1\,\beta_1) = 1$.

Sustituyendo en la ecuación anterior α y β por sus valores, y simplificando se obtiene

$$d^{2n-1}\,(\alpha\,\beta)^n = (\alpha_1 + \beta_1)\,\delta^{2n-1}$$

ahora bien; d es divisor de α y de β, por tanto será primo con δ por haber supuesto $m\,c\,d\,(\alpha\,\beta\,\delta) = 1$. Además α_1 y β_1 son primos entre sí y por tanto también lo serán $(\alpha_1\,\beta_1)^n$ y $\alpha_1 + \beta_1$, por tanto será

$$\alpha_1 + \beta_1 = d^{2n-1}$$
$$(\alpha_1\,\beta_1)^n = \delta^{2n-1}$$

y por ser $m\,c\,d\,(\alpha_1\,\beta_1) = 1$ será

$$\alpha_1 = a^{2n-1}$$
$$\beta_1 = b^{2n-1}$$

y por tanto

$$\alpha_1 + \beta_1 = d^{2n-1} = a^{2n-1} + b^{2n-1}$$

como se quería demostrar.

Teniendo en cuenta este teorema, podemos prescindir de la ecuación [II] de Fermat y dedicar nuestro esfuerzo a la ecuación [III].

6. La ecuación [III] equivale a «encontrar dos números racionales cuya suma sea igual a su producto elevado a la n-ésima potencia».

Se puede, por tanto, la ecuación [III] poner en la forma

$$x^n = \frac{1}{a} x + a \tag{IV}$$

y de esta ecuación vamos a deducir una interpretación geométrica del teorema de Fermat.

Consideremos el sistema

$$\begin{aligned} y &= x^n \\ y &= \frac{1}{a} x + a \end{aligned} \tag{π}$$

del cual por eliminación de y se obtiene la ecuación [IV] y por tanto si el teorema de Fermat es cierto, dicho sistema no admite soluciones racionales.

Consideremos la parábola

$$y^2 = 4x$$

la tangente a ésta en el punto A (x_1, y_1) es, según sabemos

$$y y_1 = 2x + 2x_1$$

siendo $x_1 = \frac{y_1^2}{4}$ por tanto

$$y y_1 = 2x + \frac{2 y_1^2}{4};$$

dividiendo por y_1, y simplificando

$$y = \frac{2}{y_1} x + \frac{y_1}{2}$$

y haciendo $\frac{2}{y_1} = \frac{1}{a}$ se obtiene

$$y = \frac{1}{a} x + a$$

que es la segunda ecuación de [π].

Siendo a racional, también lo será y_1, por ser $\frac{2}{y_1} = \frac{1}{a}$ y por tanto también será racional x_1.

La primera ecuación de [π] para todo valor de $n \gtreqqless 2$ es la ecuación de una parábola.

Por tanto «Si el teorema de Fermat es cierto, las tangentes a la parábola

$y^2 = 4x$ en los puntos racionales de ésta (exceptuando el origen) cortan a las parábolas $y = x^n$ $(n \geqq 2)$ en puntos irracionales».

Se ha demostrado (Euler) que la ecuación [II] para $n = 2$ no puede verificarse en números enteros, y según lo dicho últimamente, queda demostrado que «Las tangentes a la parábola $y^2 = 4x$ en sus puntos racionales (excepto el origen) cortan a la parábola $y = x^2$ en puntos irracionales».

7. Hagamos en [III] $xy = a$ será $x + y = a^n$ y se obtiene la ecuación

$$z^2 - a^n z + a = 0 \qquad [V]$$

Si el teorema de Fermat es cierto y a es racional, xy serán irracionales; por tanto el teorema de Fermat es equivalente al siguiente:

«*Demostrar que la ecuación* $z^2 - a^n z + a = 0$ *es irreducible en* K [1] *siendo* a *un elemento del cuerpo* $(n > 1)$.»

Desde luego la [V] es irreducible si a es un número entero.

En efecto: Para $|a| = 1$ evidentemente lo es, y si $|a| > 1$ por ser

$$|-a^n| > |a| + 1$$

según Perrón (álgebra t. II) también es irreducible.

8. Por ser irreducible la ecuación [V] no se verificará en números racionales la ecuación

$$(a^n)^2 - 4a = t^2 \qquad [VI]$$

multiplicando los dos miembros de esta por a^{2n-2} y sumando 4 se obtiene la relación

$$(a^n - 2)^2 = 4 + (t\,a^{n-1})^2.$$

Esta ecuación nos dá una interpretación geométrica del teorema de Fermat, que es la siguiente: «En todos los triángulos rectángulos racionales, teniendo un cateto de longitud dos unidades, la suma de este cateto y la hipotenusa no es una potencia $2^n - 1$ -ésima de un número racional».

9. Dividiendo los dos miembros de [VI] y por a^{2n} y haciendo $\frac{1}{a} = r$ y $\frac{t}{a^n} = y$ se obtiene la ecuación

$$1 - 4r^{2n-1} = y^2.$$

De aquí se deduce, que todas las ecuaciones cuadráticas en las cuales el radicando sea

$$1 - 4r^{2n-1} \qquad [\delta]$$

deberán ser—si el teorema de Fermat es cierto—irreducibles.

Consideremos la ecuación

$$(u_1 r^{n-1})^2 - u_1 + r = 0$$

cuyo radicando es [δ].

Si u_1 es el primer término de una progresión geométrica de razón r será $u_n = u_1 r^{n-1}$ por tanto «En todas las progresiones geométricas formadas con términos racionales, no se verifica la relación

$$u_u^2 - u_1 + r = 0 \qquad n \gtrless 2$$

siempre bajo el supuesto de que el teorema de Fermat es cierto».

10. El lector a quien le interesen estas cuestiones, puede optar por cualesquiera de las ecuaciones que hemos obtenido y por otras varias que fácilmente pueden deducirse de ellas.

Fijándonos en la ecuación [IV] se ha demostrado que no debe verificarse en números racionales, mas aún, tengo la sospecha de que el trinomio

$$x^n - \frac{1}{a} x - a \qquad [VII]$$

es irreducible en K [1] siendo a un elemento del cuerpo.

Desde luego por el teorema de Perrón se demuestra que es irreducible si $\frac{1}{a}$ es un número entero.

11. «Puesta la ecuación de Fermat en la forma [I] sea $z = a + b$ (a, b enteros) si n es primo y mayor que 2, $x\,y$ primos entre sí, y además con n el sistema

$$x^n = a^n + \binom{n}{1} b\, a^{n-1}$$

$$y^n = \binom{n}{2} b^2 a^{n-2} + \ldots\ldots + b^{n-1}$$

no puede verificarse en números enteros.»

En efecto: De la primera ecuación se deduce

$$x^n \equiv 0 \qquad (\mathrm{mod}\ a)$$

luego los divisores primos de a son divisores de x.

De la segunda ecuación se obtiene

$$y^n \equiv 0 \qquad (\mathrm{mod}\ b).$$

Por tanto los divisores primos de b lo son de y, y como por hipótesis es, $m\,c\,d\,(x, y) = 1$ se verificará $m\,c\,d\,(a, b) = 1$.

Ahora bien, a es primo con b y además con n; puesto que si n fuese divisor de a lo sería de x en contra de lo supuesto; por tanto

$$a^{n-1}, \qquad a + n.b$$

serán primos entre sí, y por tanto serán potencias n-ésimas perfectas

$$a^{n-1} = t^n \qquad a + n\,b = Y^n$$

y por ser n y $n - 1$ primos entre sí, se tendrá

$$a = X^n.$$

Se tiene pues

$$Y^n - Y^n = n\,b \tag{h}$$

siendo b primo con n, según se ha demostrado.

El segundo miembro de [h] es múltiplo de n y no lo es de n^2, y el primer miembro que es múltiplo de n forzosamente es múltiplo de n^2 lo cual es imposible; es decir, que la ecuación [h] no se verifica en números enteros y el sistema considerado tampoco, como se quería demostrar.

Número de Mersenne

12. Suponemos n primo > 3.

Sea

$$2^n - 1 = B\,C \qquad \text{B y C enteros positivos}$$

vamos a demostrar que se verifica

$$2^n \equiv B + C \qquad (\text{mod } n^2)$$

En efecto: Esta congruencia es evidente cuando es $B = 1$.

Si B y C son mayores que 1, ambos serán menores que $2^{n \;\; 1}$.

Si K y h son enteros y positivos se tendrá

$$B = 2^{n-1} - K \qquad C = 2^{n-1} - h;$$

pero por ser

$$2^{n-1} = t\,n + 1 \qquad \text{(Fermat)}$$

se obtiene

$$B = t\,n + 1 - K \qquad C = t\,n + 1 - h$$

y teniendo en cuenta el teorema fundamental de Euler (Resumen, 2.°) se verificará

$$K = n\,x \qquad h = n\,y$$

y por tanto

$$B = 2^{n-1} - n\,x \qquad C = 2^{n-1} - n\,y$$

Se tiene pues

$$2^n - 1 = B\,C = (2^{n-1} - n\,x)(2^{n-1} - n\,y) = 2^{2(n-1)} - 2^{n-1}\,n\,(x + y) + n^2\,x\,y$$

de donde

$$0 = 2^{2(n-1)} - 2^n + 1 - 2^{n-1}\,n\,(x + y) + n^2\,x\,y.$$

Teniendo en cuenta que se verifica

$$2^{2(n-1)} - 2^n + 1 = (2^{n-1} - 1)^2 \equiv 0 \qquad (\text{mod } n^2)$$

se obtiene

$$x + y \equiv 0 \qquad (\text{mod } n^2)$$

Por otra parte

$$B + C = 2^{n-1} - n\,x + 2^{n-1} - n\,y = 2^n - n\,(x + y)$$

y teniendo en cuenta la congruencia anterior se obtiene

$$B + C \equiv 2^n \qquad (\text{mod } n^2) \qquad [\delta]$$

como se quería demostrar.

13. *Forma de los divisores.*—Evidentemente se verifica

$$2^n - 1 \equiv -1 \qquad (\text{mod } 8) \qquad n > 3$$

y por lo dicho (Resumen 3.°) será

$$\left.\begin{array}{l} B = 8\,K - 1 \\ C = 8\,t + 1 \end{array}\right\} B + C = 8\,m$$

y de [δ] se deduce

$$8\,m \equiv 2^n \qquad (\text{mod } n^2)$$

simplificando

$$m = 2^{n-3} - h\,n^2. \qquad \text{[VIII]}$$

Hagamos

$$B = 2b + 1 \qquad C = 2c + 1$$

se tendrá

$$2^n - 1 = B\,C = (2b + 1)(2c + 1)$$

y de aquí

$$2^{n-1} = 2bc + b + c + 1 \qquad \text{[IX]}$$

siendo evidentemente

$$B + C = 2(b + c + 1) = 8m.$$

Por tanto

$$b + c + 1 = 4m.$$

Sustituyendo en ésta m por su valor [VIII] obtenemos

$$b + c + 1 = 4(2^{n-3} - h\,n^2). \qquad \text{[X]}$$

Eliminando $b + c + 1$ entre ésta y la [IX] y simplificando se obtiene

$$b\,c = 2\,h\,n^2 \qquad \text{[XI]}$$

siendo $C = 8t + 1 = 2c + 1$ será $c = 4t$, y por tanto [XI,

$$h = 2p$$

Sustituyendo este valor de h en la relación [X] se obtiene

$$b + c + 1 \equiv 0 \pmod 8.$$

Finalmente

$$B + C = 2(b + c + 1) \equiv 0 \pmod{16};$$

es decir: «Descompuesto $2^n - 1$ en un producto de dos factores, la suma de éstos es divisible por 16».

Consecuencia de esta propiedad y de que, según sabemos, todos los divisores de $2^n - 1$ son de la forma $8K \pm 1$, es que las dos únicas formas que pueden tener los divisores B y C de $2^n - 1$, son

$$B = 16p + 1 \qquad B = 16a + 7$$
$$C = 16q - 1 \qquad C = 16b - 7$$

no excluyendo el caso de que B valga uno.

14. *Descomposición de $2^n - 1$ en un producto de dos factores.*—De las igualdades [X] y [XI] después de sustituir h por $2\,K$ se obtiene el sistema

$$b + c = 2^{n-1} - 8\,K\,n^2 - 1$$
$$b\,c = 4\,K\,n^2$$

y de éste

$$c = \frac{2^{n-1} - 8\,K\,n^2 - 1 + \sqrt{(2^{n-1} - 8\,K\,n^2 - 1)^2 - 16\,K\,n^2}}{2}$$

$$b = \frac{2^{n-1} - 8\,K\,n^2 - 1 - \sqrt{(2^{n-1} - 8\,K\,n^2 - 1)^2 - 16\,K\,n^2}}{2},$$

valores que sustituídos en la igualdad

$$2^n - 1 = (2\,b + 1)(2\,c + 1)$$

y, simplificando, se obtiene

$$2^n - 1 = \left(2^{n-1} - 8\,K\,n^2 + \sqrt{(2^{n-1} - 8\,K\,n^2 - 1)^2 - 16\,K\,n^2}\right)\left(2^{n-1} - 8\,K\,n^2 - \right.$$
$$\left. - \sqrt{(2^{n-1} - 8\,K\,n^2 - 1)^2 - 16\,K\,n^2}\right)$$

relación que es una *identidad* de fácil comprobación.

Para $K = 0$ obtenemos

$$2^n - 1 = (2^n - 1)\,1.$$

$2^n - 1$ será compuesto, cuando exista un valor de $K > 0$ para el cual el radicando sea el cuadrado de un número entero.

Por tanto «La condición necesaria y suficiente para que el número $2^n - 1$ sea compuesto, es que se verifique en números enteros la ecuación

$$(2^{n-1} - 8\,K\,n^2 - 1)^2 - 16\,K\,n^2 = t^2 \qquad \text{[XII]}$$

siendo $K > 0$».

15. *Caso particular.*—Suponemos $K = a^2$ $t = T$, n, a, T enteros.

Sustituyendo en la [XII] K y t por sus valores y dividiendo por $a^2\,n^2$ se obtiene

$$\left(\frac{2^{n-1} - 1}{a\,n} - 8\,a\,n\right)^2 = 4^2 + T^2$$

Suponiendo existan dos enteros a y T que verifiquen a la relación últimamente obtenida, se ha de verificar evidentemente:

$$\frac{2^{n-1} - 1}{a\,n} - 8\,a\,n = \pm 5$$
$$T = \pm 3$$

y de la primera de éstas:

$$a = \frac{\pm 5 \pm \sqrt{25 + 32\,(2^{n-1} - 1)}}{16\,n} = \frac{\pm 5 \pm \sqrt{2^{n+4} - 7}}{16\,n}$$

cuando a sea entero, $2^n - 1$ será compuesto; por tanto, $2^n - 1$ será compuesto para los valores de n que verifiquen a las relaciones

$$2^{n+4} - 7 = h^2$$
$$h \equiv \pm 5 \pmod{16\,n} \qquad [XIII]$$

Estas relaciones quedan satisfechas para $n = 11$.

Comprobación:

$$2^{11+4} - 7 = 181^2$$
$$181 \equiv 5 \pmod{16 . 11}$$

16. *Estudio de la relación* $2^n - 1 = x\,(4\,x \pm 3)$.—Restando 9 de los dos miembros de la ecuación

$$2^{n+4} - 7 = h^2$$

se obtiene

$$2^{n+4} - 16 = h^2 - 9$$

y por tanto:

$$h^2 = 9 + 16\,(2^n - 1) \qquad [XIV]$$

Por otra parte las raíces de la ecuación propuesta:

$$x = \frac{\mp 3 \pm \sqrt{9 + 16\,(2^n - 1)}}{8}$$

serán racionales cuando su radicando sea un cuadrado perfecto; y como el radicando es precisamente el valor de h^2 [XIV] y de aquí que «Las raíces de la ecuación

$$2^n - 1 = x\,(4\,x \pm 3)$$

serán racionales para los valores de n para los cuales la ecuación

$$2^{n+4} - 7 = h^2$$

sea verificada en números enteros».

«Si n es primo y mayor que 3 la ecuación

$$2^n - 1 = x\,(4\,x + 3)$$

no es satisfecha en números enteros.»

En efecto: Según el teorema de Euler x y $4x+3$ serán de la forma $2Kn+1$ y se tendrá

$$4x+3=2K_1n+1=4(2Kn+1)+3=8Kn+7$$

por tanto

$$2K_1n+1=8Kn+7$$
$$(2K_1-8K)n=6$$

igualdad imposible si es $n>3$ como se quería demostrar.

Debemos, pues, considerar únicamente la ecuación

$$x(4x-3)=2^n-1 \qquad [XV]$$

cuya solución posititiva es $x=\frac{3+h}{8}$
siendo h el valor que se obtiene de la relación [XIV].

Este valor de x será entero si se verifica

$$h\equiv 5 \pmod 8.$$

Podemos enunciar la siguiente proposición: «Para los números n primos absolutos y mayores que 3 tales que la relación

$$2^{n+4}-7=h^2$$

sea verificada en números enteros, siendo

$$h\equiv 5 \pmod 8$$

2^n-1 será compuesto y su descomposición factorial será de la forma $x(4x-3)$».

17. *Estudios de la relación* [XV] *para valores de* n *primos* $\geqq 11$.

Según hemos demostrado (13), de la relación [XV] se deduce

$$x+4x-3=5x-3\equiv 0 \pmod{16} \qquad [\omega]$$

siendo

$$\left.\begin{array}{l} x\equiv \pm 1 \\ x\equiv \pm 7 \end{array}\right\} \pmod{16}$$

y de estos números el único que satisface a $[\omega]$ es 7; por tanto será

$$x=16m+7$$

sustituyendo en [XV] y simplificando

$$(16m+7)(64m+25)=2^n-1 \qquad [\tau]$$

Efectuando operaciones

$$2^{n-4}=2^6m^2+53m+11.$$

Los valores de m que verifican a esta relación son de la forma $m=64t+1$.
Sustituyendo en [τ] y simplificando

$$2^n-1=(2^{10}t+23)(2^{12}t+89) \qquad [\tau']$$

Ahora bien; por ser $1+23.89=2^{11}$ y, además, haber supuesto $n \geqq 11$, será $2^n-1-23.89$ divisible por 2^{11}, por tanto es $t=2z$.
Sustituyendo en la igualdad [τ′] se obtiene finalmente

$$2^n-1=(2^{11}z+23)(2^{13}z+89) \qquad [XVI]$$

que es la descomposición factorial para todo valor de n primo $\geqq 11$ y para el cual las relaciones

$$2^{n+4}-7=h^2$$
$$h \equiv 5 \pmod 8$$

sean satisfechas con números enteros.
Habiendo deducido la relación [XVI] de la ecuación

$$2^n-1=x(4x-3)$$

y siendo condición necesaria para que esta ecuación sea satisfecha en números enteros que lo sea la ecuación

$$2^{n+4}-7=h^2$$

resulta que para todo valor de n primo para el cual la relación anterior no es satisfecha en números enteros, 2^n-1 no admite la descomposición [XVI].

18. *Estudio de la ecuación* $2^{n+4}-7=h^2$.

Restando 5 de los dos miembros de la ecuación

$$2^{n+4}-7=h^2 \qquad [\varepsilon].$$

se obtiene

$$2^2(2^{n+2}-3)=h^2-5$$

esta ecuación y por tanto la [ε] no serán verificadas en números enteros para los números n, tales que si p es es un número primo de la forma $10\,m \pm 3$ se verifique

$$2^{n+2} - 3 \equiv 0 \pmod{p}$$

puesto que para estos números p no se verifica (Resumen 4.°)

$$h^2 - 5 \equiv 0 \pmod{p}$$

Sea p un número primo de la forma $10\,m \pm 3$ y supongamos se verifica

$$2^y - 3 \equiv 0 \pmod{p}$$

siendo y el menor número que verifica a la congruencia; sea g el gaussiano.

Evidentemente

$$2^{y+gk} - 3 \equiv 0 \pmod{p} \qquad K = 1, 2, \ldots\ldots$$

Hagamos

$$n + 2 = y + g\,k;$$

por tanto

$$n = y + g\,k - 2.$$

Si n es un número primo deducido de esta expresión, la [ε] no es verificada en números enteros para este valor de n, y, por tanto $2^n - 1$ no admite la descomposición factorial [XVI].

Ejemplos:

1.° $\qquad p = 23 \;\;,,\;\; 2^8 - 3 \equiv 0 \pmod{23} \qquad g = 11.$

y de los infinitos números primos que se deducen de la fórmula

$$n = 8 + 11\,K - 2 = 6 + 11\,K \qquad (K = 1, 2, \ldots\ldots)$$

figuran

$$n = 17, 61, 83, 127, 149, 281, 347, 457, 479, 677, 743, 787, 809, 853, 919, 941, \ldots\ldots$$

Para estos valores de n la expresión $2^n - 1$ o bien es un número primo, o bien es compuesto, pero en este caso no admite la descomposición [XVI].

2.° $\qquad p = 53 \quad y = 17 \quad g = 52 \;\;,,\;\; n = 15 + 52\,K$

$\qquad p = 97 \quad y = 19 \quad g = 48 \quad n = 17 + 48\,K$

para $K = 5$ se obtiene:

$$n = 17 + 48.5 = 257.$$

Se sabe que $2^{257} - 1$ es compuesto, pero no se conoce su descomposición factorial; nosotros podemos asegurar que no es la [XVI].

Por otro procedimiento podemos obtener infinitos números primos n para los cuales la relación [ε] no es verificada en números enteros; es el siguiente: Restemos 25 de los miembros de [ε], se obtiene:

$$2^5(2^{n-1}-1)=h^2-25.$$

Si el segundo miembro es múltiplo de 5 lo será de 25. Considerando los números n tales que $2^{n-1}-1$ sea divisible por 5 y no lo sea por 25, la última ecuación, y, por tanto, la [ε] no serán verificadas en números enteros.

Estos números son los que satisfacen a las relaciones:

$$n-1=4\,\mathrm{K}, \quad m\,c\,d\,(\mathrm{K},5)=1$$

puesto que si $2^{n-1}-1$ ha de ser múltiplo de 25, $n-1$ tiene que ser divisible por 20.

Por tanto, «2^n-1 no admite la descomposición factorial [XVI] si n es primo de la forma $4\,\mathrm{K}+1$ y no termina en 1».

Las soluciones enteras y positivas que nosotros conocemos de la ecuación [ε] son:

1.ª	$n=0$	$h=3$	$2^4-7=3^2$
2.ª	$n=1$	$h=5$	$2^5-7=5^2$
3.ª	$n=3$	$h=11$	$2^7-7=11^2$
4.ª	$n=11$	$h=181$	$2^{15}-7=181^2$

De estas cuatro soluciones, solamente esta última, o sea para $n=11$, 2^n-1 es compuesto y admite la descomposición [XVI] siendo, como es sabido,

$$2^{11}-1=23.89.$$

la descomposición factorial obtenida de [XVI] haciendo $z=0$.