SOBRE EL TEOREMA DE FERMAT

DE QUE LA ECUACION $x^n+y^n=z^n$ NO TIENE SOLUCION EN NÚMEROS ENTEROS x, y, z I SIENDO n>2

(Conclusion)

III

Recordamos que hemos hecho las trasformaciones de H_0', espresadas en (25) i (27), con el objeto de poder determinar con mayor facilidad la congruencia (16)

$$H'_0 \equiv 0 \bmod n,$$

para los dos casos de $n\equiv 1$ i $n\equiv 2$ mod 3. Se tratará de demostrar jeneralmente, en cuanto sea posible, que no puede tener lugar la congruencia $H'_0\equiv 0$ mod n en ninguno de los casos mencionados.

Necesitamos valernos para esto de un teorema, perteneciente a la teoria de las "formas binarias cuadráticas" (**********) diciendo:

"Que por la forma binaria cuadrática

$$(2, 1, 2)=2x^2+2xy+2y^2$$

(**********) Véanse «*Vorlesungen über Zahlentheorie von P. G. Lejeune—Dirichlet*, 3^te^ *Auflage* § *70*» o cualquier tratado de la teoria de los números.

Luego será, en el caso de $n \equiv 1 \bmod 3$, para

$$g^2 + gh + h^2 \equiv 0 \bmod n,$$

segun (24),

$$H_0' = (a^2 + ab + b^2)^2 \psi[(a+b)^2, ab] \equiv 0 \bmod n^4 \qquad (31)$$

Resulta, pues, de la forma (12') de la ecuacion (12), a saber:

$$nab\left\{H_0 + H_1 G + H_2 G^2 + \ldots + H_{n-3} G^{n-3} + H_{n-2} G^{n-3}\right\} = G^n$$

que debe ser o H_1 divisible por una potencia de n o G divisible por n^4.

Todavia no he podido decidir la cuestion respecto a la suposicion $G \equiv 0 \bmod n^4$, caso que reservaré, por esto, para mas tarde.

En vez de esto vamos a demostrar, que no tiene lugar la congruencia

$$H_1 \equiv 0 \bmod n.$$

Segun la ecuacion (12), es

$$\left.\begin{aligned} H_1 = {} & (n-1)(a^{n-3} + b^{n-3}) + \frac{(n-1)(n-2)}{2!} ab(a^{n-5} + b^{n-5}) + \\ & + \frac{(n-1)(n-2)(n-3)}{3!} (ab)^2 (a^{n-7} + b^{n-7}) + \ldots\ldots + \\ & + \frac{(n-1)(n-2)\ldots(n-\frac{n-3}{2})}{(\frac{n-3}{2})!} (ab)^{\frac{n-5}{2}} (a^2 + b^2) + \\ & + \frac{(n-1)(n-2)\ldots(n-\frac{n-1}{2})}{(\frac{n-1}{2})!} (ab)^{\frac{n-3}{2}} \end{aligned}\right\} \qquad (32)$$

Para averiguar si H_1 es o no divisible por n, transformamos a (32) en una congruencia segun el módulo n, aprovechando

$$a^2 + ab + b^2 \equiv 0 \bmod n,$$

congruencia de la cual deducimos facilmente las siguientes segun mod n

$$a^2+b^2\equiv -ab$$
$$a^4+b^4=(a^2+b^2)^2-2a^2b^2\equiv -(ab)^2$$
$$a^6+b^6=(a^2+b^2)(a^4+b^4)-a^2b^2(a^2+b^2)\equiv 2(ab)^3$$
$$a^8+b^8=(a^4+b^4)^2-2a^4b^4\equiv -(ab)^4$$

o jeneralmente

$$\left.\begin{aligned} &a^{2r}+b^{2r}\equiv -(ab)^r \text{ siendo } r\equiv 1,\ 2 \bmod 3\\ &a^{2r}+b^{2r}\equiv 0 \qquad\quad \text{siendo } r\equiv 0 \bmod 3\end{aligned}\right\} \quad (33)$$

Tomando como comprobado ésto hasta cierto valor $s\equiv 1 \bmod 3$, así que se tienen,

$$a^{2s}+b^{2s}\equiv -(ab)^s,\ a^{2(s-1)}+b^{2(s-1)}\equiv 2(ab)^{s-1}$$

por ser $s-1\equiv 0 \bmod 3$, se siguen

$$a^{2(s+1)}+b^{2(s+1)}=(a^2+b^2)(a^{2s}+b^{2s})-a^2b^2(a^{2(s-1)}+b^{2(s-1)})\equiv (ab)^{s+1}$$

i

$$a^{2(s+2)}+b^{2(s+2)}=(a^2+b^2)(a^{2(s+1)}+b^{2(s+1)})-a^2b^2(a^{2s}+b^{2s})\equiv 2(ab)^{s+2},$$

en fin,

$$a^{2(s+3)}+b^{2(s+3)}=(a^2+b^2)(a^{2(s+2)}+b^{2(s+2)})-$$
$$-a^2b^2(a^{2(s+1)}+b^{2(s+1)})\equiv -(ab)^{s+3}$$

Por lo tanto, demostradas las congruencias (33) hasta $s=4$, ellas valen jeneralmente.

Ahora bien, siendo $n=3\nu+1=6\nu'+1$, $\frac{n-3}{2}=3\nu'-1\equiv 2 \bmod 3$, $\frac{n-5}{2}=3\nu'-2\equiv 1 \bmod 3$, $\frac{n-7}{2}=3\nu'-3\equiv 0 \bmod 3$ etc., se tiene por medio de (33):

$$H_1\equiv (ab)^{\frac{n-3}{2}}\left\{-(n-1)-\frac{(n-1)(n-2)}{2!}+\right.$$
$$+2\frac{(n-1)(n-2)(n-3)}{3!}\mp\ldots\ldots\ldots-$$
$$\left.-\frac{(n-1)(n-2)\ldots(n-\frac{n-3}{2})}{(\frac{n-3}{2})!}+\frac{(n-1)(n-2)\ldots(n-\frac{n-1}{2})}{(\frac{n-1}{2})!}\right\} \bmod n$$

Para efectuar la adición de la serie, tenemos que distinguir entre 4 clases de términos

$$1)\quad \frac{(n-1)(n-2)\ldots[n-(3u+1)]}{(3u+1)!}=\frac{n.\ U+(-1)^{3u+1}.\ (3u+1)!}{(3u+1)!}.$$

Puesto que un tal término tiene que ser número entero, será $U\equiv 0 \bmod (3u+1)!$ i, por eso,

$$\frac{n.\ U+(-1)^{3u+1}.(3u+1)!}{(3u+1)!}\equiv(-1)^{3u+1} \bmod n$$

i, por la misma razon, es

$$2)\quad \frac{(n-1)(n-2)\ldots.[n-(3u+2)]}{(3u+2)!}\equiv(-1)^{3u+2} \bmod n.$$

Nótese que la suma de los dos términos es $\equiv 0 \bmod n$.

$$3)\quad 2\frac{(n-1)(n-2)\ldots.[n-(3u+3)]}{(3u+3)!}\equiv 2(-1)^{3u+3} \bmod n,$$

en fin, el último término

$$4)\quad \frac{(n-1)(n-2)\ldots(n-\frac{n-1}{2})}{(\frac{n-1}{2})!}\equiv(-1)^{\frac{n-1}{2}} \bmod n.$$

Encontrándose ahora en la serie (34) los términos de las dos primeras clases a pares, o sea un término de la primera siempre seguido por uno de la segunda, así que en suma se destruyen, en cuanto a su congruencia mod n, se convierte (34) en la congruencia que sigue

$$H_1\equiv(ab)^{\frac{n-3}{2}}\left\{2\sum_{u=1}^{\frac{n-7}{6}}(-1)^{3u}+(-1)^{\frac{n-1}{2}}\right\} \bmod n$$

Hai que distinguir aquí entre 2 casos

1.º $\frac{n-1}{2}=3\nu'\equiv 0 \bmod 2$

Sea $\frac{n-1}{2}=6\nu''$, será $\frac{n-7}{6}=2\nu''-1\equiv 1 \bmod 2$ i, por eso,

$$H_1\equiv(ab)^{\frac{n-3}{2}}(-2+1)\equiv-(ab)^{\frac{n-3}{2}} \bmod n$$

2.º $\frac{n-1}{2}=3\nu'\equiv 1 \bmod 2$

Sea $\frac{n-1}{2}=6\nu''+3$, será $\frac{n-7}{2}=2\nu''\equiv 0 \bmod 2$ i, por consiguiente,

$$H_1\equiv(ab)^{\frac{n-3}{2}}(0-1)\equiv-(ab)^{\frac{n-3}{2}} \bmod n$$

Tenemos, por lo tanto, siempre

$$H_1\equiv-(ab)^{\frac{n-3}{2}} \bmod n$$

pero, por saber ya, desde páj. 286, que ni a ni b pueden ser divisible por n, no puede ser tampoco

$$H_1\equiv 0 \bmod n$$

Este resultado, en combinacion con lo dicho anteriormente (pájina 418), dá a conocer que, siendo

$$n\equiv 1 \bmod 3 \text{ i } a^2+ab+b^2\equiv 0 \bmod n^2$$

es necesario para la existencia de la ecuacion (12) que G sea divisible por n^4, caso que escluimos todavia de la consideracion.

A no ser $a^2+ab+b^2\equiv 0 \bmod n^2$, sea para $n\equiv 1 \bmod 3$ ó sea, como debe ser siempre, para $n\equiv 2 \bmod 3$, se necesita demostrar que no hai valores de a i b que puedan satisfacer a las congruencias

$$\psi[(a+b)^2, ab]\equiv 0 \bmod n \text{ para } n\equiv 1 \bmod 3$$

o $$\psi_1[(a+b)^2, ab]\equiv 0 \bmod n \text{ para } n\equiv 2 \bmod 3,$$

lo que va a ser objeto del párrafo siguiente.

IV

Volvamos a apuntar en primer lugar los valores de ψ i ψ_1 espresados en las ecuaciones (24) hasta (27), i en las formas siguientes:

Para $n \equiv 1 \bmod 3$

$$\psi[(a+b)^2, ab] = [(a+b)^2 - ab]^{\frac{n-7}{2}} +$$

$$+ \sum_{r=1}^{\frac{n-7}{6}} \frac{[n-(2r+3)][n-(2r+5)]\ldots\ldots[n-(6r+1)]}{2^{2r}(2r+1)!} \times$$

$$\times (ab)^{2r}(a+b)^{2r}[(a+b)^2 - ab]^{\frac{n-7}{2}-3r}$$

Para $n \equiv 2 \bmod 3$

$$\psi_1[(a+b)^2, ab] = [(a+b)^2 - ab]^{\frac{n-5}{2}} +$$

$$+ \sum_{r=1}^{\frac{n-5}{6}} \frac{[n-(2r+3)][n-(2r+5)]\ldots[n-(6r+1)]}{2^{2r}(2r+1)!} \times$$

$$\times (ab)^{2r}(a+b)^{2r}[(a+b)^2 - ab]^{\frac{n-5}{2}-3r}$$

No daremos en adelante la demostracion de que ni ψ ni ψ_1 son $\equiv 0 \bmod n$, en fórmulas jenerales, sino consideraremos casos especiales de n. Sin embargo vamos a establecer algunos puntos de vista jenerales con el objeto de facilitar i simplificar el cálculo especial.

En las líneas siguientes se entienden las congruencias segun el módulo n, a no ser que se esprese formalmente otro módulo. Los puntos mencionados son los cinco siguientes:

1.) Encontrándose en las funciones ψ i ψ_1 a i b solo bajo las formas $(a+b)^2$ i ab, simétricas respecto a a i b, basta considerar una sola de las 2 combinaciones posibles ab i ba de los valores de a i b.

2.) Por la misma razon, dá $a \equiv \eta_1$, $b \equiv \eta_2$ el mismo resultado que $a \equiv -\eta_1$, $b \equiv -\eta_2$, como tambien $a \equiv \eta_1$, $b \equiv -\eta_2$ i $a \equiv \eta_2$, $b \equiv -\eta_1$ dan lo mismo.

3.) Siendo $a \equiv \delta.a_1$, $b \equiv \delta.b_1$, donde δ significa un número entero, positivo o negativo, menor que n, se pueden sentar

$$\psi \equiv \delta^{n-7}\left\{[(a_1+b_1)^2 - a_1b_1]^{\frac{n-7}{2}} + \sum_{r=1}^{\frac{n-7}{2}} \frac{[n-(2r+3)]..[n-(6r+1)]}{2^{2r}(2r+1)!} \times \right.$$

$$\left. \times (a_1b_1)^{2r}(a_1+b_1)^{2r}[(a_1+b_1)^2 - a_1b_1]^{\frac{n-7}{2}-3r} \right\}$$

i

$$\psi_1 \equiv \delta^{n-5}\left\{[(a_1+b_1)^2-a_1b_1]^{\frac{n-5}{2}}+\sum_{r=1}^{\frac{n-5}{6}}\frac{[n-(2r+3)]\,[n-(6r+1)]}{2^{2r}(2r+1)!}\times\right.$$

$$\left.\times(a_1b_1)^{2r}(a_1+b_1)^{2r}[(a_1+b_1)^2-a_1b_1)^{\frac{n-5}{2}-3r}\right\}$$

Ahora es claro que δ, como número menor que n, no puede ser $\equiv 0 \bmod n$, por eso, se reducen las congruencias $\psi \equiv 0$ i $\psi_1 \equiv 0$, para a i b, a análogas, para las magnitudes menores a_1 i b_1.

4) De los puntos anteriores, 1, 2 i 3, se desprende ademas un procedimiento que hace posible la reduccion de los valores de a a tales que sean $\equiv 1 \bmod n$. Se sabe que un residuo impar $\pm r$, segun el módulo impar n, puede ser sustituido por un residuo par $\mp(n-r)$, igual al complemento de r respecto a n, con signo contrario. Formados de tal manera 2 residuos pares, en lugar de a i b, se puede sustituir estos, segun punto 3, por otros, enjendrados por medio de division por 2 o por una potencia de 2. Siguiendo, respecto a los valores resultantes, del mismo modo, es decir, trasformándolos i dividiéndolos, en seguida, por la mayor potencia posible de 2, puede bien suceder que resulte, despues de un número finito de operaciones, para a o b un valor $\equiv 1 \bmod n$. A no sucederlo, es necesario que se reproduzca, por el procedimiento indicado, el mismo número del cual se ha partido, i en este caso se tendría que buscar otras divisiones, fuera del 2, para reducir, finalmente, uno de los valores correspondientes a a o b a la unidad lo que parece ejecutable en cada caso.

Espuesto lo anterior podemos, pues, formar respecto a cada n, para cualquier número $<n$, ciertas series de números, averiguando así, si el número conduce o no a ± 1. Si la serie contiene a ∓ 1, es claro que basta considerar, en este caso, a $\equiv 1 \bmod n$, i si la serie reproduce el mismo número, con signo + o −, de que se ha partido, sin que se obtenga antes la unidad, se necesitará un cálculo especial para la reduccion propuesta, cálculo que efectuaremos mas abajo. Se entiende, de antemano, que no

hai necesidad de considerar, en el último caso, a congruente a un número par ni congruente a un número mayor que $\frac{n-1}{2}$. Tambien es claro que de las series mencionadas quedan escluidas, desde luego, las potencias de 2.

5) Siendo $a \equiv 1 \bmod n$, se encuentra para

$$b \equiv \tfrac{n-1}{2} - \epsilon$$

$$(a+b)^2 - ab \equiv (\tfrac{n+1}{2} - \epsilon)^2 - (\tfrac{n-1}{2} - \epsilon)(\tfrac{n+1}{2} - \epsilon) \equiv \tfrac{n+1}{2}\cdot\tfrac{n+3}{2} + \epsilon^2$$

i
$$ab(a+b) \equiv (\tfrac{n-1}{2} - \epsilon)(\tfrac{n+1}{2} - \epsilon) \equiv \frac{n^2-1}{4} + \epsilon^2$$

i para
$$b \equiv \tfrac{n-1}{2} + \epsilon$$

$$(a+b)^2 - ab \equiv (\tfrac{n+1}{2} + \epsilon)^2 - (\tfrac{n-1}{2} + \epsilon)(\tfrac{n+1}{2} + \epsilon) \equiv \tfrac{n+1}{2}\cdot\tfrac{n+3}{2} + \epsilon^2$$

i
$$ab(a+b) \equiv (\tfrac{n-1}{2} + \epsilon)(\tfrac{n+1}{2} + \epsilon) \equiv \frac{n^2-1}{4} + \epsilon^2$$

Por lo tanto, resultan para ψ i ψ_1 las mismas congruencias mod. n, sea $b \equiv \frac{n-1}{2} - \epsilon$ o $\equiv \frac{n-1}{2} + \epsilon$.

Basta, por consiguiente, considerar para b solamente los valores $\equiv 1, 2, \ldots \frac{n-1}{2}$.

Fuera de estas 5 reglas jenerales hai en algunos casos especiales otras modificaciones del cálculo las que indicaremos oportunamente.— De antemano se entiende que, mientras mas grande es n, mas complicado será el cálculo. Para mayor claridad pondremos, por eso, desde $n = 11$, cuadros en los cuales aparecen los varios valores de b i de los otros términos uno al lado del otro i los que pertenecen al mismo valor de b uno debajo del otro.

Volvemos a advertir que en los casos de $n \equiv 1 \bmod 3$ no se cuenta con valores correspondientes a

$$a^2 + ab + b^2 = (a+b)^2 - ab \equiv 0 \bmod n.$$

Daremos, en fin, demostraciones para algunos valores de n.

1) n = 5 ≡ 2 mod 3

Encontramos $\psi_1 = 1$ que no es$\equiv 0 \bmod 5$.

$$2)\ n = 7 \equiv 1 \bmod 3$$

$\psi_2 = 1$ no puede ser, por esto, $\psi \equiv 0 \bmod 7$

$$3)\ n = 11 \equiv 2 \bmod 3$$

$$\psi_1 = [(a+b)^2 - ab]^3 + \frac{6.4}{2.^2\ 3!}(ab)^2(a+b)^2_4$$

o $$\psi_1 = [(a+b)^2 - ab]^3 + [ab(a+b)]^2$$

Formemos la serie, por medio del procedimiento, esplicado en punto 4, indicando por una raya vertical que separa a dos números, la aplicacion de los puntos 1, 2 o 3.

La serie será

$$5 \equiv -6 \mid -3 \equiv 8 \mid 1,$$

serie que contiene, como se vé, a todos los números impares i menores o iguales a $\frac{n-1}{2} = 5$ o sean 5, 3, 1. Basta, por lo tanto, considerar $a \equiv 1$, i segun punto 5, $b \equiv 1, 2, 3, 4, 5 \bmod 11$
$a \equiv 1 \bmod 11$ hace

$$\psi_1 \equiv [(1+b)^2 - b]^3 + [b(1+b)]^2 \bmod 11$$

Siendo especialmente $[b(1+b)]^2$ un número cuadrado, no puede ser, como residuo cuadrático de 11, sino

$$\equiv 1, -2, 3, 4, 5$$

i, por eso, no hai necesidad de considerar valores de b que hacen ni a $[(1+b)^2 - b]^3$ ni, por consecuencia, a

$$(1+b)^2 - b \equiv 1, -2, 3, 4, 5, \qquad (35)$$

porque la suma de dos residuos cuadráticos, respecto a un módulo n que sea $\equiv 3 \bmod 4$, nunca es $\equiv 0 \bmod n$.

Encontrándose, pues, en el cuadro siguiente una de las congruencias (35) (como en verdad sucede con 3 i -2) no calculamos a ψ_1. Ahora es segun mod 11

$b \equiv$	1	2	3	4	5
$(1+b)^2-b \equiv$	3	-4	2	-1	-2
$[(1+b)^2-b]^3 \equiv$		2	-3	-1	
$[b(1+b)]^2 \equiv$		3	1	4	
$\psi_1 \equiv$		5	-2	3	

Ninguna vez tenemos $\psi_1 \equiv 0 \bmod 11$.

4) n = 13 ≡ 1 mod 3

$$\psi = [(a+b)^2-ab]^3 + \frac{8.6}{2.^2 3!}[ab(a+b)]^2 = [(a+b)^2-ab]^3 + 2[ab(a+b)]^2$$

La serie

$$3 \equiv -10 \mid -5 \equiv 8 \mid 1$$

contiene a todos los números impares i $< \frac{n-1}{2} = 6$, por eso, se consideran $a \equiv 1$, i, segun punto 5, $b \equiv 1, 2, 3, 4, 5, 6 \bmod 13$:

$a \equiv 1 \bmod 13$ dá

$$\psi = [(1+b)^2-b]^3 + 2[b(1+b)]^2$$

No siendo aquí $2[b(1+b)]^2$ un residuo cuadrático de 13, puesto que 2 no lo es, será

$$2[b(1+b)] \equiv \pm 2, \pm 5, \pm 6$$

i, por eso, no se necesita tomar en cuenta valores de b que dan

$$(1+b)^2 - b \pm \equiv 1, \pm 3, \pm 4$$

Tenemos

$b \equiv$	1	2	3	4	5	6
$(1+b)^2-b \equiv$	3	-6	0	-5	5	4
$[(1+b)^2-b]^3 \equiv$		5		5	-5	
$2[b(1+b)]^2 \equiv$		-6		-6	6	
$\psi \equiv$		-1		-1	1	

Ningun valor de b dá, por lo tanto, $\psi \equiv 0 \bmod 13$.

5) $n = 17 \equiv 2 \bmod 3$

La serie

$$3 \equiv -14 \mid -7 \equiv 10 \mid 5 \equiv -12 \mid -3$$

dá a conocer que ni 7 ni 5 ni 3 conducen a la unidad, pero las combinaciones siguientes demuestran que, sin embargo, basta tomar $a \equiv 1 \bmod 17$. A saber

1) $\begin{array}{c|c|c|c} a \equiv 3 \equiv 3 & 1 & a \equiv 3 \equiv -14 & -2 \\ b \equiv 5 \equiv -12 & -4' & b \equiv 7 \equiv 7 & 1 \end{array} \quad \begin{array}{c} 1 \\ -2 \end{array}$

2) $\begin{array}{c|c|c|c} a \equiv 5 \equiv -12 & -2 & 1 & a \equiv 5 \equiv 5 \\ b \equiv 6 \equiv 6 & 1 & -2' & b \equiv 7 \equiv -10 \end{array} \quad \begin{array}{c} 1 \\ -2 \end{array}$

Para $a \equiv 1$, $b \equiv 1, 2, 3, 4, 5, 6, 7, 8 \bmod 17$ se convierte

$$\psi_1 = [(a+b)^2 - ab]^6 + \frac{12.10}{2^2.3!}(ab)^2(a+b)^2[(a+b)^2-ab]^3 +$$

$$+ \frac{10.8.6.4}{2^4.5!}(ab)^4(a+b)^4$$

en

$$\psi_1 \equiv [(1+b)^2-b]^6 + 5[b(1+b)]^2[(1+b)^2-b]^3 + [b(1+b)]^4$$

$$\equiv \left\{ [(+b)^2-b]^3 + [b(1+b)]^2 \right\}^2 + 3[b(1+b)]^2[(1+b)^2-b]^3$$

Pongamos abreviadamente, en este caso, como en los siguientes,

$$(1+b)^2-b=a,\ b(1+b)=\beta$$

¡ será

$$\psi_1\equiv(a^3+\beta^2)^2+3a^3\beta^2$$

i por ser, como residuo cuadrático de 17,

$$(a^3+\beta^2)^2\equiv\pm1,\ \pm2,\ \pm4,\ \pm8$$

se deja a un lado los valores de b que hacen a

$$3a^3\beta^2\equiv\pm3,\ \pm5,\ \pm6,\ \pm7$$

Luego resulta el siguiente cuadro de congruencias mod 17

$b\equiv$	1	2	3	4	5	6	7	8
$a^3\equiv$	-7	3	4	-4	7	-2	-5	6
$\beta^2\equiv$	4	2	8	-8	-1	-4	8	-1
$3a^3\beta^2\equiv$	1	1	-6	-6	-4	7	-1	-1
$(a^3+\beta^2)^2\equiv$	-8	8			2		-8	8
$\psi_1\equiv$	-7	-8			-2		8	7

No hai, como se vé, valores de b que satisfacen a $\psi_1\equiv0$ mod 17.

6) n=19≡1 mod 3

La serie

$$9\equiv-10\ |\ -5\equiv14\ |\ 7\equiv-12\ |\ -3\equiv16\ |\ 1$$

indica, por contener, a 9, 7, 5, 3, que es suficiente considerar $a \equiv 1 \bmod 19$. Tenemos, por consiguiente, $a \equiv 1$, $b \equiv 1, 2, 3, 4, 5, 6, 7, 8, 9 \bmod 19$.

$$\psi = [(a+b)^2 - ab]^6 + \frac{14.12}{2^2.3!}[ab(a+b)]^2[(a+b)^2 - ab]^3 +$$

$$+ \frac{12.10.8.6}{2^4.5!}[ab(a+b)]^4$$

$$\equiv [(1+b)^2 - b]^6 + 7[b(1+b)]^2[(1+b)^2 - b]^3 + 3[b(1+b)]^4$$

Las sustituciones

$$(1+b)^2 - b = a,\ b(1+b) = \beta$$

hacen a

$$\psi \equiv a^6 + 7a^3\beta^2 + 3\beta^4$$

Siendo, como residuo cuadrático,

$$a^6 \equiv 1, -2, -3, 4, 5, 6, 7, -8, +9$$

no hai que tomar en consideracion valores de b que hacen a $7a^3\beta^2 + 3\beta^4$ congruente a esos números

El cuadro será aquí

$b \equiv$	1	2	3	4	5	6	7	9	9
$a^3 \equiv$	8	1	−7	8	−1	−8	0	−8	−7
$\beta^2 \equiv$	4	−2	−8	1	7	−3		−3	6
$7a^3\beta^2 \equiv$	−4	5	−7	−1	8	−3		−3	−9
$3\beta^4 \equiv$	−9	−7	2	3	−5	8		8	−6
$7a^3\beta^2 + 3\beta^4 \equiv$	6	−2	−5	2	3	5		5	4
$a^6 \equiv$			−8	7	1				
$\psi \equiv$			6	9	4				

No aparece $\psi \equiv 0 \bmod 19$.

7) $n = 23 \equiv 2 \bmod 3$

La serie

$$11 \equiv 12 \mid -3 \equiv 20 \mid 5 \equiv -18 \mid -9 \equiv 14 \mid 7 \equiv -16 \mid -1$$

contiene a todos los números impares $\leq \frac{n-1}{2} = 11$. Consideremos, pues,

$$a \equiv 1; b \equiv 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11 \bmod 23.$$

$$\psi_1 \equiv [(a+b)^2 - ab]^9 + \frac{18.16}{2^2.3!}[ab(a+b)]^2[(a+b)^2 - ab]^6 +$$

$$+ \frac{16.14.12.10}{2^4.5!}[ab(a+b)]^4[(a+b)^2 - ab]^3 +$$

$$+ \frac{14.12.10.8.6.4}{2^6.7!}[ab(a+b)]^6$$

$$\equiv [(1+b)^2 - b]^9 + 12[b(1+b)]^2[(1+b)^2 - b]^6 +$$

$$+ 14[b(1+b)]^4[(a+b)^2 - b]^3 + [b(1+b)]^6$$

$$\equiv a^9 + 12a^6\beta^2 + 14a^3\beta^4 + \beta^6$$

Por ser el residuo cuadrático

$$\beta^6 \equiv 1, 2, 3, 4, -5, 6, -7, 8, 9, -10, -11$$

no debe ser congruente a los mismos números el término

$$a^9 + 12a^6\beta^2 + 14a^3\beta^4 = \psi_1 - \beta^6$$

Por lo tanto, tenemos el cuadro

$b\equiv$ 1	2	3	4	5	6	7	8	9	10	11
$a^3\equiv$ 4	−2	−11	−8	6	−4	−3	−5	−1	5	−10
$\beta^2\equiv$ 4	−10	6	9	3	−7	8	9	4	2	−10
$14a^3\beta^4\equiv$ −1	6	−1	−10	−3	−7	3	11	6	4	7
$12a^6\beta^2\equiv$ 9	3	−5	−11	8	−10	−10	9	2	2	6
$a^9\equiv$ −5	−8	3	−6	9	5	−4	−10	−1	10	−11
$\psi_1-\beta^6\equiv$ 3	1	−3	−4	−9	11	−11	10	7	−7	2
$\beta^6\equiv$		9	−7	4	2		−7	−5		
$\psi_1\equiv$		6	−11	−5	−10		3	2		

No se encuentra $\psi_1\equiv 0 \bmod 23$.

8) $n = 29 \equiv 2 \bmod 3$

Aquí tenemos la serie

$$7\equiv -22\,|\,-11\equiv 18\,|\,9\equiv -20\,|\,-5\equiv 24\,|\,3\equiv -26\,|\,-13\equiv 16\,|\,1,$$

por la que queda demostrado que basta considerar $a\equiv 1 \bmod 29$, puesto que aparecen en ella todos los números impares i $<\frac{n-1}{3}=14$. Tomemos, pues, $a\equiv 1$; $b\equiv 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, \bmod 29$.

$$\psi_1=[(a+b)^2-ab]^{12}+\frac{24.22}{2^2.3!}[ab(a+b)]^2\,[(a+b)^2-ab]^9+$$

$$+\frac{22.20.18.16}{2^4.5!}[ab(a+b)]^4\,[(a+b)^2-ab]^6+$$

$$+\frac{20.\ 18.\ 16.\ 14.\ 12.\ 10}{2^6.\ 7!}[ab(a+b)]^6[(a+b)^2-ab]^3+$$

$$+\frac{18.\ 16.\ 14.\ 12.\ 10.\ 8.\ 6.\ 4}{2^2.\ 9!}[ab(a+b)]^8$$

$$\equiv[(1+b)^2-b]^{12}+22[b(1+b)]^2[(1+b)^2-b]^9+$$

$$+66[b(1+b)]^4[(1+b)^2-b]^6+$$

$$+30[b(1+b)]^6[(1+b)^2-b]^3+[b(1+b)]^8$$

$$\equiv a^{12}-7a^9\beta^2+8a^6\beta^4+a^3\beta^6+\beta^8\equiv(a^6+\beta^4)^2-7a^9\beta^2+$$

$$+6a^6\beta^4+a^3\beta^6$$

Por el residuo cuadrático $(a^6+\beta^4)^2$ el que es

$$\equiv\pm1,\ \pm4,\ \pm5,\ \pm6,\ \pm7,\ \pm9,\ \pm13$$

no se necesitan considerar los valores de b que dan

$$A=-7a^9\beta^2+6a^6\beta^4+a^3\beta^6\equiv\pm2,\ \pm3,\ \pm8,\ \pm10,\ \pm11,$$

$$\pm12,\ \pm14.$$

Luego será:

$b \equiv$	1	2	3	4	5	6	7	8	9	10	11	12	13	14
$a^3 \equiv$	2	− 5	− 7	10	8	−11	− 1	11	6	− 9	12	−12	4	−10
$\beta^2 \equiv$	4	7	− 1	− 6	1	− 5	4	− 7	9	7	− 5	5	6	− 9
$-7a^1\beta^2 \equiv$	− 8	6	6	8	12	−11	− 1	− 2	− 7	− 7	−14	−14	9	−12
$6a^6\beta^4 \equiv$	7	13	4	− 5	7	− 4	9	− 9	9	5	− 5	− 5	5	− 4
$a^3\beta^6 \equiv$	−12	− 4	7	−14	8	12	− 6	− 3	− 5	−13	8	8	− 6	11
$A \equiv$	−13	−14	−12	−11	− 2	− 3	2	−14	− 3	14	−11	−11	8	− 5
$(a^6+\beta^4)^2 \equiv$	− 6													− 9
$\psi_1 \equiv$	10													−14

Tampoco en este caso no hai ninguna vez $\psi_1 \equiv 0 \bmod 29$.

9) $n = 31 \equiv 1 \bmod 3$

Obtenemos, en este caso, 3 series diferentes, a saber

$$15 \equiv -16 \mid -1;\ 13 \equiv -18 \mid -9 \equiv 22 \mid 11 \equiv -20 \mid -5 \equiv 26 \mid 13;$$

$$7 \equiv -24 \mid -3 \equiv 28 \mid 7$$

Los números impares, 13, 11, 9, 7, 5, 3 que forman parte de las 2 últimas series, requieren consideraciones especiales, respecto a las reducciones propuestas. Encontramos

1) $a \equiv 3 \equiv -28 \mid -14 \equiv -14 \mid -7 \equiv 24 \mid 8 \equiv 8 \mid 2 \equiv 2 \mid 1$
$b \equiv 5 \equiv -26 \mid -13 \equiv 18 \mid 9 \equiv 9 \mid 3 \equiv -28 \mid -7 \equiv 24 \mid 12'$

$a \equiv 3 \equiv 3 \mid 1$
$b \equiv 7 \equiv -24 \mid -8'$

$a \equiv 3 \equiv -28 \mid -14 \equiv -14 \mid -7 \equiv 24 \mid 4 \equiv 4 \mid 1$
$b \equiv 10 \equiv 10 \mid 5 \equiv -26 \mid -13 \equiv 18 \mid 3 \equiv -28 \mid -7'$

$a \equiv 3 \equiv -28 \mid -7 \equiv 24 \mid 12 \equiv 12 \mid -2 \equiv 2 \mid 1$
$b \equiv 11 \equiv -20 \mid -5 \equiv 26 \mid 13 \equiv -18 \mid -3 \equiv 28 \mid 14'$

$a \equiv 3 \equiv 3 \mid 1$ $a \equiv 3 \equiv -28 \mid -2 \mid 1$
$b \equiv 13 \equiv -18 \mid -6'$ $b \equiv 14 \equiv 14 \mid 1 \mid -2$

2) $a \equiv 5 \equiv -26 \mid -13 \equiv 18 \mid 6 \mid 1$
$b \equiv 6 \equiv 6 \mid 3 \equiv 3 \mid 1 \mid 6'$

$a \equiv 5 \equiv -26 \mid -13 \equiv 18 \mid 3 \equiv -28 \mid -14 \mid 1$
$b \equiv 7 \equiv -24 \mid -12 \equiv -12 \mid -2 \equiv -2 \mid -1 \mid 14'$

$a \equiv 5 - 26 \mid -13 \equiv 18 \mid 9 \equiv 9 \mid 3 \equiv 3 \mid 1$ $a \equiv 5 \equiv 5 \mid 1$
$b \equiv 9 - 22 \mid -11 \equiv 20 \mid 10 \equiv -21 \mid -7 \equiv 24 \mid 8'$ $b \equiv 11 \equiv -20 \mid -4'$

$a \equiv 5 \equiv -26 \mid -13 \equiv 18 \mid 3 \mid 1$ $a \equiv 5 \equiv -26 \mid -2 \mid 1$
$b \equiv 12 \equiv 12 \mid 6 \equiv 6 \mid 1 \mid 3'$ $b \equiv 13 \equiv 13 \mid 1 \mid -2'$

$a \equiv 5 \equiv -26 \mid -13 \equiv 18 \mid 3 \equiv -28 \mid -7 \mid 1$
$b \equiv 14 \equiv 14 \mid 7 \equiv -24 \mid -4 \equiv -4 \mid -1 \mid 7$

3) $a \equiv 7 \equiv -24 \mid -8 \equiv -8 \mid -2 \equiv -2 \mid -1 \mid 1$
$b \equiv 9 \equiv 9 \mid 3 \equiv -28 \mid -7 \equiv 24 \mid 12 \mid -12'$

$a \equiv 7 \equiv 7 \mid 1$ $a \equiv 7 \equiv -24 \mid -6 \equiv -6 \mid -3 \equiv -3 \mid -1 \mid 1$
$b \equiv 10 \equiv -21 \mid -3'$ $b \equiv 11 \equiv -20 \mid -5 \equiv 26 \mid 13 \equiv -18 \mid -6 \mid 6'$

$a \equiv 7 \equiv -24 \mid -2 \mid 1$ $a \equiv 7 \equiv -26 \mid -2 \mid 1$
$b \equiv 12 \equiv 12 \mid 1 \mid -2'$ $b \equiv 13 \equiv 13 \mid 1 \mid -2$

4) $\begin{matrix} a\equiv 9 & \equiv & 9 & | & 3\equiv 3 & | & 1 \\ b\equiv 10 & \equiv & -21 & | & -7\equiv 24 & | & 8' \end{matrix}$ $\begin{matrix} a\equiv 9 & \equiv & -22 & | & -2 & | & 1 \\ b\equiv 11 & \equiv & 11 & | & 1 & | & -2' \end{matrix}$

$\begin{matrix} a\equiv 9 & \equiv & -22 & | & -11\equiv & 20 & | & 5\equiv -26 & | & -13\equiv & 18 & | & 6 & | & -1 \\ b\equiv 14 & \equiv & 14 & | & 7 & \equiv -24 & | & -6\equiv -6 & | & -3 & \equiv -3 & | & -1 & | & 6 \end{matrix}$

5) $\begin{matrix} a\equiv 11 & \equiv & -20 & | & -5 \\ b\equiv 12 & \equiv & 12 & | & 3 \end{matrix}$ se reduce a $\begin{matrix} a\equiv 3 \\ b\equiv 5 \end{matrix}$

$\begin{matrix} a\equiv 11 & \equiv & -20 & | & -10 \\ b\equiv 13 & \equiv & -18 & | & -9 \end{matrix}$ se reduce a $\begin{matrix} a\equiv 9 \\ b\equiv 10 \end{matrix}$

$\begin{matrix} a\equiv 11 & \equiv & -20 & | & -10 \\ b\equiv 14 & \equiv & 14 & | & 7 \end{matrix}$ se reduce a $\begin{matrix} a\equiv 7 \\ b\equiv 10 \end{matrix}$

6) $\begin{matrix} a\equiv 13 & \equiv & -18 & | & -9 \\ b\equiv 14 & \equiv & 14 & | & 7 \end{matrix}$ se reduce a $\begin{matrix} a\equiv 7 \\ b\equiv 9 \end{matrix}$

Por lo tanto basta considerar

$$a\equiv 1;\ b\equiv 1,\ 2,\ 3,\ 4,\ 5,\ 6,\ 7,\ 8,\ 9,\ 10,\ 11,\ 12,\ 13,\ 14,\ 15.$$

$$\psi=[(a+b)^2-ab]^{12}+\frac{26.24}{2^2.3!}[ab(a+b)]^2[(a+b)^2-ab]^9+$$

$$+\frac{24.22.20.18}{2^4.5!}[ab(a+b)]^4[(a+b)^2-ab]^6+$$

$$+\frac{22.20.18.16.14.12}{2^6.7!}[ab(a+b)]^6[(a+b)^2-ab]^3+$$

$$+\frac{20.18.16.14.12.10.8.6}{2^8.9!}[ab(a+b)]^8$$

$$\equiv[(1+b)^2-b]^{12}+26[b(1+b)]^2[(1+b)^2-b]^9+99[b(1+b)]^4\times$$

$$\times[(1+b)]^2-b]^6+66[b(1+b)]^6[(1+b)^2-b]^3+5[b(1+b)]^8$$

$$\equiv a^{12}-5a^9\beta^2+6a^6\beta^4+4a^3\beta^6+5\beta^8\equiv(a^3+\beta^2)^4-9a^9\beta^2+4\beta^8$$

Siendo, como residuo cuadrático,

$$(a^3+\beta^2)^4\equiv 1,\ 2,-3,\ 4,\ 5,-6,\ 7,\ 8,\ 9,\ 10,-11,-12,-13\ 14,-15,$$

no debe ser congruente a estos números el término

$$A=-9\ a^9\beta^2+4\ \beta^8$$

Se encuentra aquí el cuadro siguiente:

$b\equiv$	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
$\alpha^3\equiv$	−4	2	4	−8	0	−8	−1	−2	−8	4	−15	8	4	1	−2
$\beta^2\equiv$	4	5	−11	−3		−3	5	7	9	10	2	1	−15	−13	2
$-9\alpha^9\beta^2\equiv$	10	12	−12	2		2	14	8	−6	6	−10	11	−9	−7	−11
$4\beta^8\equiv$	1	−11	5	−5		−5	−11	−6	−13	10	2	4	8	9	2
$A\equiv$	11	1	−7	3		−3	3	2	12	−15	−8	15	−1	2	−9
$(\alpha^3+\beta^2)^4\equiv$	0		2				8		1		10	−11	9		0
$\psi\equiv$	11		−5				11		13		2	4	8		−9

Ningun valor de b hace $\psi\equiv 0 \bmod 31$.

Demostrado así, en algunos casos especiales, que ni ψ ni ψ_1 pueden ser$\equiv 0 \bmod n$, resulta que no existen, respecto a éstos,

valores enteros de a, b i G que podrian satisfacer a la ecuacion (12) ni, por eso, valores enteros de x, y, z capaces a llenar la ecuacion (1) de que se trata

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

salvo todavia el caso de que seria

$$a^2 + ab + b^2 \equiv 0 \mod n.$$

Siempre se ha dado la demostracion completa del teorema de Fermat en cuestion para

$$n = 3, 5, 11, 17, 23 \text{ i } 29,$$

quedando todavia pendiente, considerar la congruencia

$$G \equiv 0 \mod n^4$$

para

$$n = 7, 13, 19 \text{ i } 31.$$

DR. A. TAFELMACHER
Profesor de matemáticas del Instituto Pedagójico

Santiago de Chile, Agosto 27 de 1892.