ALGUNAS NOTICIAS SOBRE EL ULTIMO TEOREMA DE FERMAT

Jorge Vargas

Aproximadamente en 1637, Fermat conjeturó que no existen naturales no nulos x,y,z que resuelven la ecuación $x^n + y^n = z^n$ $n > 2$, fijo. Hasta hoy en día nadie ha podido probar o negar la conjetura de Fermat. Sin embargo, esta pregunta ha generado un tremendo avance del conocimiento matemático, lo que ha permitido dar respuestas parciales y positivas a la conjetura. Para describir estas respuestas necesitamos una definición: Diremos que una terna de enteros x,y,z, cada uno de ellos no nulos, es una solucion primitiva de la ecuación de Fermat de orden n si

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

El máximo común divisor de x,y,z es uno

Ejercicio. Probar que toda solución entera no trivial (x,y,z) de $X^n + Y^n = Z^n$ (es decir $xyz \neq 0$) es un múltiplo entero de una solución primitiva.

-Probar que resolver la conjetura de Fermat para n equivale a probar que la ecuación $X^n + Y^n = Z^n$ no tiene soluciones primitivas.

Un teorema de G. Faltings en Endlichkeitssätze für abelsche Varietätn uber Zahlkörpen, Inv. Math., 73 (1983). 349-366 establece:

Para cada exponente $n \geq 3$, la ecuación $X^n + Y^n = Z^n$ tiene a lo sumo un número finito de soluciones primitivas.

Por otro lado, Wagstaff en The irregular primes to 125.000 Math. Comp., 32 (1978), 583-591 recopile y completa

la prueba de que la conjetura de Fermat es verdadera para $n \leq 125.000$.

Ejercicio: Si todo número natural primo fuera menor a 125.000, la conjetura de Fermat se duduciría del trabajo de Wagstaff.

Ejercicio: Si se conociera la validez de la conjetura de Fermat para $n = 4$ y para todo primo $p \geq 3$, entonces la conjetura de Fermat sería verdadera para todo natural mayor o igual a tres.

Una pregunta que surge es ¿Cómo se ataca una resolución de la conjetura de Fermat? En el caso de Faltings, lo que en realidad hizo, fue resolver una conjetura hecha por Mordell en la década del 30 de la cual se deduce la afirmación de Fermat. ¡Convertir el problema en un caso particular de un problema más general!

Otro posible ataque es el siguiente:

Sea $D = \{p: p \text{ primo}, x^p + y^p = z^p$ no tiene soluciones primitivas x,y,z tal que p es coprimo al producto $xyz\}$.

Sea $B = \{p$ primo, $x^p + y^p = z^p$ no tiene soluciones primitivas x,y,z tal que p divide al producto $xyz\}$.

Notar: $p \in D \cap B$ si y solo si la conjetura de Fermat es válida para p.

$D \cap B$ = totalidad de primos mayor o igual a 3 si y solo si la conjetura de Fermat es verdadera.

De acuerdo a Wagstaff todo primo distinto de dos y menor a 125.000 pertenece a $D \cap B$.

Teorema. Si p es primo y $p < 6.10^9$ entonces p pertenece a D.

Para una demostración consultar Lehner. On Fermat's quotient, base two, Math. Comp. 36 (1981) 289-290.

Teorema. (Sophie German, 1832) Si p es primo y 2p+1 es primo, entonces p pertenece a D

Ejercicio: Escribir un programa de computadora que produzca los primeros cien números primos p tal que 2p+1 es primo.

Corolario 3,5,11 pertenecen a D.

Teorema. D es infinito.

Para una prueba consultar Adleman, Fouvry and Heath-Brown, Inv. Math. 79 (1985), 409-416.

Ellos prueban para x grande vale que

$$\text{Cardinal } \{p \in D: p \leq x\} \geq cx^{2/3}$$

donde c es positivo y no depende de x, es un fácil ejercicio, que esta desigualdad implica la infinitud de D.

Problema abierto: ¿El número de primos p tal que 2p+1 es primo es finito o infinito?

Problema abierto: ¿Es B infinito?

Finalmente haremos un razonamiento heurístico que permite concluir que existirán primos fuera de D.

Teorema. (Wieferich-Mirimanoff)

$p \in D$ salvo que

$$2^{p-1} \equiv 1 \bmod (p^2)$$
$$3^{p-1} \equiv 1 \bmod (p^2)$$

se satisfacen simultáneamente.

Hasta principios de 1985, no se conocía ningún primo p tal que $2^{p-1} \equiv (p^2)$ y $3^{p-1} \equiv 1\ (p^2)$ y parecería (si Fermat afirmó correctamente) que no existen tales primos.

Se sabe, verificado con una computadora, que para $p \leq 6.10^9$ sólo p = 1093 y p = 3511 resuelven $2^{p-1} \equiv 1\ (p^2)$.

Al final, escribimos una demostración de $2^{1092} \equiv 1$

(1093^2). Veamos ahora que probablemente existen números primos p que satisfacen ambas ecuaciones $2^{p-1} \equiv 1(p^2)$ y $3^{p-1} \equiv 1\ (p^2)$.

Por el pequeño teorema de Fermat sabemos existen naturales a,b tal que

$$2^{p-1} = 1 + ap, \qquad 3^{p-1} = 1 + bp$$

Además, se esperaría que los residuos módulo p de a estarían equitativamente distribuidos, por lo tanto la probabilidad de que p/a sería 1/p. De esto, la probabilidad de que p/a y p/b sería $1/p^2$. De modo que la probabilidad L de que existan números primos p que son solución de ambas congruencias sería

$$L = \frac{1}{2^2} + \frac{1}{3^2} + \frac{1}{5^2} + \frac{1}{7^2} + \frac{1}{11^2} + \quad = \sum_{p \geq 2} \frac{1}{p^2}$$

¡la suma es sobre todo los primos!

Este número L satisface que $0,36 < L < 1$.

La primera desigualdad sale de $L > \frac{1}{2^2} + \frac{1}{3^2} > 0,36$ Usando una computadora y el programa adjunto para $N = 1000$ se prueba que $L < 1$ de la manera siguiente. Por un lado tenemos que:

$$L - \sum_{p \leq N} 1/p^2 = \sum_{p \geq (N+1)} 1/p^2 \leq \sum_{n \geq (N+1)} 1/n^2$$

Aqui, $\sum_p$ indica suma sobre los primos p tal que...

Aqui, $\sum_n$ indica suma sobre todos los naturales n tal que...

Ahora, $\int_N^\infty 1/x^2\ dx$ es la area debajo de la curva $y = 1/x^2$ entre N e infinito. La cual es mayor que $\sum_{n=N+1}^{\infty} 1/n^2$. Pero $\int_N^\infty 1/x^2\ dx = \frac{1}{N}$. De esto, $L - \sum_{p \leq N} 1/p^2 \leq \frac{1}{N}$. De modo que

$$L \leq \sum_{p \leq 1000} 1/p^2 + 0,001 \simeq 0.4521205 + 0,001 = 0,4531205$$

Por lo tanto $L < 1$. En consecuencia hay probabilidad que exista un primo fuera de D pero no certeza!

En el libro Introduction to Theory of Numbers de Hardy y Wright se encuentre la igualdad

$$\sum_{P=2}^{\infty} 1/p^2 = \int_2^{\infty} \frac{1}{t^2}\, c(t)dt$$

(suma sobre los primos)

donde $c(t) = \sum_{\substack{p \le t \\ p \text{ primo}}} 1/p = \ln(t) + \tau(t)$ con $\tau(t)$ acotada, pero el autor no sabe que hacer con esta identidad.

Verificación de $2^{1092} \equiv (1093^2)$

Sea $q = 1093$, por tanto $q^2 = 1194649$. Ahora $3^7 = 2187 = 2q+1$ por tanto (*) $3^{14} \equiv 4q+1 \ (q^2)$. Como $2^{14}=16384= 15q-11$, resulta $2^{28} \equiv -330q + 121 \ (q^2)$

De esto, (Las congruencias son mod q^2)

$$3^2\, 2^{28} \equiv -2970q + 1089 = -2969q-4 \equiv -1876q-4$$

en consecuencia (dividiendo por 4) resulta

$$3^2 2^{26} \equiv -469q-1$$

Por binomio de Newton resulta

$3^{14}\, 2^{182} \equiv -(469q + 1)^7 \equiv -3283\, q-1$ y por tanto $3^{14}\, 2^{182} \equiv -4q-1$ (**)

Por (*) y (**) sigue que

$3^{14}\, 2^{182} \equiv -3^{14}$, $2^{182} \equiv -1$ y $2^{1092} \equiv 1 \bmod (1093^2)$.

Ejercicio: Probar que si $x = (r^2-s^2)c$, $y = 2rsc$ $z = (r^2+s^2)c$ con r,s,c enteros, entonces (x,y,z) es solución de $x^2 + y^2 = z^2$ y que toda solución entera de $x^2 + y^2 = z^2$ se

lo escribe de esta manera para r,s,c enteros convenientemente elegidos.

```
100 Rem "Este programa calcula la suma S de 1/p^2 para p
    primo entre 2 y N".
110 Input "Deme N=?":N
120 S = 0.25
130 For K = 3 to N
140 Let Z = INT (SQR(K))
150 For I = 2 to Z
160 Let R = K - I*INT(K/I)
170 If R = 0 then 200
175 goto 180
180 next I
185 PRINT "LOS PRIMOS ENTRE 3 Y ";N;"SON"
187 Print K
190 S = S+(1/k^2)
200 next K
210 print "S=";S
```

Bibliografía:

Heath-Brown, The first case of Fermat's last theorem. The Mathematical Intelligencer, Vol 7 # 4, 1985.

Facultad de Matemática, Astronomía y Física
Valparaíso y Rogelio Martínez -
Ciudad Universitaria - Córdoba