Es imposible descomponer un cubo en dos cubos.

Trabajo Fin de Grado

Departamento de Algebra.

Enrique Barragán Borja

Dirigido por: Francisco Javier Calderón Moreno.

Universidad de Sevilla.
Facultad de Matemáticas.

Índice general

Abstract

The objective of this work is to study the proof of Fermat's last theorem. We study some trivial cases of Fermat's last theorem, Sophie Germain's theorem, which established the first case of Fermat's theorem, and we also study the local and modular Fermat problem.

Finally, we will focus on the proof of Fermat's last theorem by using elliptic curves, modular forms and the Shimura-Taniyama conjecture.

To study all these problems, we have used differents techniques of algebraic number theory, elliptic curves, modular functions, L-functions and Galois representations.

Capítulo 0

Introducción

En el margen de su copia de la edicion de Bachet de los trabajos de Diofante, Pierre de Fermat, uno de los principales matemáticos del siglo XVII, escribió:

"Cubum autem in duos cubos, aut quadratoquadratum in duos quadratoquadratos, et generaliter nullam in infinitum ultra quadratum potestatem in duos eiusdem nominis fas est dividere cuius rei demonstrationem mirabilem sane detexi, hanc marginis exiguitas non caperet."

"Es imposible encontrar la forma de convertir un cubo en la suma de dos cubos, una potencia cuarta en la suma de dos potencias cuartas, o en general cualquier potencia más alta que el cuadrado, en la suma de dos potencias de la misma clase. He descubierto para el hecho una demostración excelente. Pero este margen es demasiado pequeño para que quepa en él."

Este enunciado se conoce como el *último teorema de Fermat*:

Si n es cualquier número natural mayor que 2, la ecuación

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

no tiene solución en los enteros distintos de 0.

En este trabajo, vamos a ir desarrollando las pruebas que diversos matemáticos realizaron para el teorema de Fermat: desde casos particulares, pasando por el primer caso del teorema de Fermat, hasta el final donde K. Ribet y A. Wiles lograron probar casi 400 años despues el teorema de Fermat y la conjetura de Shimura-Taniyama. Debido a la gran cantidad de matemáticos interesados en demostrar dicho teorema, estos intentos de la prueba han desarrollado muchísimo el area de la teoría algebraica de números.

Para empezar nos servimos de varios resultados de teoría algebraica de números para probar el teorema de Fermat en los casos particulares donde el exponente $n = 2$, $n = 4$,

$n = 3$, $n = 5$ y $n = 7$, donde en todos se llega a la misma conclusión: no existe solución de la ecuación de Fermat distinta de la trivial.

Posteriormente, Sophie Germain, matemática francesa del siglo XVIII dio una demostración para el primer caso del teorema de Fermat en 1823. El primer caso dice lo siguiente:

Teorema 1 *Sean x, y, z enteros no nulos, p primo tales que p divide a xyz se tiene que la ecuación $x^p + y^p + z^p \equiv 0 \ (mod\ p)$ no tiene solución excepto la trivial.*

Dicha prueba se estableció para cada primo $p < 100$ aunque posteriormente, Legendre, Dickson y Vandiver (entre otros) consiguieron probar el teorema de Sophie Germain para cada primo $p < 7000$. Por último, Kapferer en 1964 y Powell en 1978, independientemente, probaron que bajo unas ciertas condiciones, existe un conjunto infinito de exponentes primos entre sí para los que el primer caso del teorema de Fermat es cierto.

A continuación, para poder entender el problema local y modular de Fermat, damos una serie de resultados que tienen que ver con el cuerpo de los números p-ádicos, los polinomios con coeficientes p-ádicos y, por último, el lema de Hensel, probado por Hensel en 1908, que afirma la existencia, bajo condiciones adecuadas, de raices p-ádicas de polinomios. Este lema nos servirá para probar que para cada primo q, la ecuación de Fermat tiene solución en los enteros q-ádicos.

Por último, expondremos el razonamiento para demostrar el teorema de Fermat. Para ello realizamos un estudio previo de conceptos necesarios para la prueba. Primero hablaremos de las curvas de Frey, que son un tipo particular de curvas elípticas semiestables, con propiedades muy útiles para trabajar con ellas. Posteriormente, introduciremos el concepto de forma modular, que es una funcion holomorfa en el semiplano superior que verifica

$$f(z) = f(z+1), \quad f(z) = (cz+d)^2 f\left(\frac{az+d}{cz+d}\right) \text{ para toda } \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_0(N)$$

donde $\Gamma_0(N)$ es un subgrupo de $SL_2(\mathbb{Z})$ que cumple que c es divisible por N, es decir, el subgrupo de las matrices con determinante 1 en las que c es divisible por N. Al ser éstas funciones periódicas, tienen un desarrollo de Fourier $f(z) = \sum_{n=0}^{\infty} c_n e^{2\pi i n z}$ y son estos c_n los que a menudo aportan información aritmética.
A continuación, comentamos la conjetura de Shimura-Taniyama:

Teorema 2 (Shimura-Taniyama) *Toda curva elíptica sobre $\mathbb{Q}$ es modular.*

Esencialmente, establece que si N_p es el número de puntos de una curva elíptica sobre $\mathbb{Q}$ al considerarla módulo p, siendo p primo, entonces existe una forma modular de peso 2 $f(z) = \sum_{n=0}^{\infty} c_n e^{2\pi i n z}$ con ciertas características tal que sus coeficientes de Fourier c_p coinciden con N_p. Se dice entonces que la curva elíptica es modular. K. Ribet, con ayuda de B. Mazur, demostró en 1986 que la curva de Frey no puede ser parametrizada por

funciones modulares. De este modo, la conjetura implicaba la no existencias de soluciones de Fermat. Posteriormente, A. Wiles en 1993 presentó una prueba de la conjetura de Shimura-Taniyama que era erronea, pero en 1995, con ayuda de R. Taylor demostró la conjetura para curvas elípticas semiestables, condición suficiente para probar el último teorema de Fermat. Dicha variante dice:

Teorema 3 *Toda curva elíptica semiestable con coeficientes racionales es modular.*

En 1999, la conjetura fue probada en su totalidad por C. Breuil, B. Conrad, F. Diamond y R. Taylor.

Finalmente, vemos la prueba por reducción al absurdo de K. Ribet del teorema de Fermat. Busca la contradicción entre la conjetura de Shimura-Taniyama y el teorema de Ribet. Dicho teorema dice lo siguiente:

Teorema 4 *Si hay una solución (x, y, z, n) de la ecuación de Fermat, entonces la curva elíptica definida por la ecuación*

$$y^2 = x(x - A)(x + B)$$

donde A y B se definen como en la curva de Frey, es semiestable pero no modular

La prueba se basa en el método de descenso de nivel que afirma que bajo las condiciones adecuadas hay una autoforma de un nivel mas bajo que da esencialmente la misma representación de Galois. Este proceso puede ser repetido tanto como N tenga factores primos impares. Es importante que la curva E sea semiestable para que asi N sea libre de cuadrados. Esto dice que los factores primos impares de N pueden ser eliminados, así que debe haber una autoforma no trivial de nivel 2, es decir, en $S(2)$ esto da la misma representacion de Galois. Y esto es una contradicción entre la conjetura de Shimura-Taniyama y el teorema de Ribet.

Capítulo 1

Casos especiales

En el primer capítulo vamos a probar los casos del teorema de Fermat para exponentes 2, 4, 3, 5 y 7. Empezaremos por el exponente 2.

1.1. La ecuación pitagórica

Estudiaremos brevemente la ecuación pitagorica:

$$x^2 + y^2 = z^2 \tag{1.1}$$

Euclides ya dio una versión geométrica para encontrar soluciones. Fibonacci también dio un método para encontrar todas las soluciones, pero fue Diofante el que encontró un método para encontrar todas las soluciones. Dicho resultado es:

(1A) *Sean $a, b \in \mathbb{Z}$ tales que $a > b > 0$, m.c.d.$(a, b) = 1$ y con a y b de diferente paridad, entonces la terna (x, y, z) dada por:*

$$\begin{cases} x = 2ab \\ y = a^2 - b^2 \\ z = a^2 + b^2 \end{cases}$$

es una solución primitiva de (1.1). Esto establece una correspondencia biyectiva entre el conjunto de pares (a, b) satisfaciendo la condición anterior, y el conjunto de soluciones primitivas de (1.1).

Observando (1A), encontrar soluciones primitivas de (1.1) equivale a determinar qué enteros impares positivos son suma de dos cuadrados y, en cada caso, escribir todas sus representaciones. Fermat probó que $n > 0$ es suma de dos enteros al cuadrado si y solo si cada factor primo p de n, tal que $p \equiv 3$ $(mod\ 4)$, aparece como una potencia par en la descomposición de n en factores primos.
Llamemos $r(n)$ al número de pares ordenados (a, b) tales que $a^2 + b^2 = n$ con n, a, b enteros. Por ejemplo: $r(1) = 4$, $r(5) = 8$.

Jacobi y Gauss independientemente probaron: $r(n) = 4(d_1(n) - d_3(n))$ con $d_1(n)$, respectivamente $d_3(n)$, el número de divisores de n congruentes con 1 módulo 4, respectivamente, congruentes a 3 en módulo 4.
De este modo, podemos determinar las primitivas (x, y, z). Para la prueba utilizaremos la siguiente identidad:

$$(a^2 + b^2)(c^2 + d^2) = (ac + bd)^2 + (ad - bc)^2 = (ac - bd)^2 + (ad + bc)^2 \tag{1.2}$$

En 1908, Botari dio otra parametrización para las soluciones de (1.1) y cuya prueba realizo Cattaneo:

(1B) *Si a y b son números naturales impares tal que $m.c.d(a, b) = 1$, si $s \geq 1$ entonces la terna (x, y, z) dada por:*

$$\begin{cases} x = 2^{(2s-1)}a^2 + 2^s ab \\ y = b^2 + 2^s ab \\ z = 2^{(2s-1)}a^2 + b^2 + 2^s ab \end{cases}$$

es una solución primitiva de (1.1). Esto establece una correspondencia biyectiva entre el conjunto de ternas (a, b, s) satisfaciendo la condición anterior y el conjunto de soluciones primitivas de (1.1).

1.2. La ecuación bicuadrática

Veamos ahora el caso $n = 4$. Fermat consideró el problema de si el área de un triángulo pitagórico podría ser el cuadrado de un entero. Por tanto, estudió la ecuación:

$$x^4 - y^4 = z^2 \tag{1.3}$$

y postuló:

(1C) *La ecuación (1.3) no tiene solución en los enteros distintinta de la solución nula.*

En lo que concluye con el siguiente corolario:

(1D) *El área de un triángulo pitagórico no es cuadrado de un entero.*

Además, se obtiene:

(1E) *La ecuación*

$$x^4 + y^4 = z^4 \tag{1.4}$$

no tiene soluciónes no nulas en los enteros.

Con estos resultados, Euler probó:

(1F) *La ecuación*

$$x^4 + y^4 = z^2 \tag{1.5}$$

no tiene soluciónes no nulas en los enteros.

Otros autores dieron la prueba para este caso $n = 4$. Veamos el resultado de Vranceanu:

(1G) *Son equivalentes:*

1. *El último teorema de Fermat para exponente $n = 4$ es cierto.*
2. *Para todo entero $m \neq 0$ las únicas soluciones no nulas en los enteros de $2x^4 = my(m^2 + y^2)$ son (m, m) y $(-m, m)$.*

1.3. La ecuación de quinto grado

La solución del caso $n = 5$ fue propuesta por primera vez por Dirichlet en 1825, pero su prueba, la cual dio en 1828, no consideraba todos los casos. Vamos a reproducir la prueba de Dirichlet en lenguaje moderno usando algunos aspectos del campo $K = \mathbb{Q}(5)$. Sea A el anillo de los enteros de $\mathbb{Q}(5)$. Los elementos de A tienen la forma $(a+b\sqrt{5})/2$ con a,b enteros de la misma paridad. Las unidades de A (es decir, los elementos invertibles de A) forman un grupo multiplicativo. $(a + b\sqrt{5})/2$ es una unidad si y solo si su norma

$$\left(\frac{a + b\sqrt{5}}{2}\right)\left(\frac{a - b\sqrt{5}}{2}\right) = \frac{a^2 - 5b^2}{4}$$

es igual a ± 1, es decir, las unidades de A son los elementos $\pm\left((1 + \sqrt{5})/2\right)^e$ con e entero. Vamos a establecer una propiedad de ciertos ideales principales de A que son potencias quintas:

(1H)

1. *Sean a,b enteros no nulos tales que $m.c.d.(a, b) = 1$, $a \not\equiv b \ (mod\ 2)$, $5 \not| \ a$, $5 \mid b$. Si $a^2 - 5b^2$ es la quinta potencia de un elemento de A entonces existen unos enteros c,d no nulos, tales que:*

$$\begin{cases} a = c(c^4 + 50c^2d^2 + 125d^4) \\ b = 5d(c^4 + 10c^2d^2 + 5d^4) \end{cases} \tag{1.6}$$

y $m.c.d.(c, d) = 1$, $c \not\equiv b \ (mod\ 2)$, $5 \not| \ c$.

2. *Sean a,b enteros, tales que m.c.d.*$(a,b)=1$*, ambos impares,* $5 \not| a$, $5 \mid b$. *Si* $\dfrac{a^2-5b^2}{4}$ *es la quinta potencia de un elemento de A entonces existen unos enteros c,d no nulos, tales que:*

$$\begin{cases} a = c(c^4+50c^2d^2+125d^4)/16 \\ b = 5d(c^4+10c^2d^2+5d^4)/16 \end{cases} \tag{1.7}$$

y m.c.d.$(c,d)=1$*, ambos impares,* $5 \not| c$.

(1I) *La ecuación*

$$x^5+y^5+z^5=0 \tag{1.8}$$

no tiene solucion en los enteros distinta de 0.

En 1912, Plenelj provó la extensión del anterior teorema, al igual que hizo Nagell (1958):

(1J) *La ecuación*

$$x^5+y^5+z^5=0 \tag{1.9}$$

solo tiene la solución trivial en enteros del cuerpo $\mathbb{Q}(\sqrt{5})$.

1.4. La ecuación de séptimo grado

En 1839, Lamé probó el teorema de Fermat de exponente $n=7$. Lebesgue encontró una prueba más simple en 1840 y, a su vez, Genocchi diseñó una prueba más simple aún en 1874 y 1876 usando una idea de Legendre (1830), reproducida en el libro de Nagell (1951):

(1K)

1. *Si x,y,z son las raices de una ecuación cúbica con coeficientes en* $\mathbb{Q}$*, tales que* $x^7+y^7+z^7=0$*, entonces* $xyz=0$ *ó x,y,z son proporcionales a las raices cúbicas de* 1*, las cuales son* 1, $\xi=(-1+\sqrt{-3})/2$, $\xi^2=(-1-\sqrt{-3})/2$.

2. *La ecuación* $x^7+y^7+z^7=0$ *sólo tiene la solución trivial en los enteros.*

Capítulo 2

Teorema de Sophie Germain

Para empezar, enunciaremos el primer caso del teorema de Fermat:

(2A) *Sean x, y, z enteros no nulos, p primo tales que $p \mid xyz$ se tiene que la ecuación $x^p + y^p + z^p \equiv 0 \ (mod\ p)$ no tiene solución excepto la trivial.*

En este capítulo daremos una prueba del teorema de Sophie Germain para el primer caso del teorema de Fermat. Sophie Germain, matemática francesa, probó un teorema que estableció el primer caso del teorema de Fermat para cada primo $p < 100$. Empezaremos con esta observación, la cual fue dada también por Bang en 1935:

(2B) *Sea q primo, $n \geq 3$ un entero impar. Entonces son equivalentes:*

1. *Existen enteros a, b, c, no múltiplos de q, tales que $a^n + b^n + c^n \equiv 0 \ (mod\ q)$.*
2. *Existen enteros d, e, no múltiplos de q, tales que $d^n \equiv e^n + 1 \ (mod\ q)$. Además, si $q - 1 = 2kn$, las afirmaciones anteriores son equivalentes a:*
3. *Existen raices u, v de $x^{2k} - 1 \equiv 0 \ (mod\ q)$ tales que $v \equiv u + 1 \ (mod\ q)$.*

Ahora daremos la versión de Legendre del teorema de Sophie Germain:

(2C) *Sean p, q primos impares distintos y suponiendo que se cumplen las condiciones:*

1. *Si a, b, c son enteros tales que $a^p + b^p + c^p \equiv 0 \ (mod\ q)$ entonces $q \mid abc$.*
2. *p no es congruente módulo q con la p-ésima potencia de un entero.*

Entonces el primer caso del teorema de Fermat es cierto para el exponente p.
Seguido de otro resultado:

(2D) *Si p, q son primos impares tales que $q - 1 = 2pk$, donde k es un número natural, entonces la segunda condición de (**2C**) es equivalente a las siguientes:*

1. *$(2k)^{2k} \not\equiv 1 \ (mod\ q)$; y*

2. $p^{2k} \not\equiv 1 \ (mod\ q)$.

El siguiente corolario del del teorema de Sophie Germain dice:

(2E) *Si* p *es un primo impar y* $q = 2p + 1$ *es primo también, entonces el primer caso del teorema de Fermat es cierto para el exponente* p.

Además, Legendre amplió este criterio en 1823:

(2F) *Si* p *es un primo impar y* $q = 4p + 1$, $q = 8p + 1$, $q = 10p + 1$, $q = 14p + 1$ *ó* $q = 16p + 1$ *es también primo, entonces el primer caso del teorema de Fermat es cierto para el exponente* p.

Con este criterio, Legendre había probado que el primer caso del teorema de Fermat es cierto para cada exponente primo $p < 197$. La única limitación fue la longitud de los números involucrados. En 1897, Maillet extendió este resultado hasta $p = 211$ y Mirimanoff, en 1905, lo amplió hasta $p = 257$ usando un método que introducía números de Bernoulli. En 1908, Dickson probó usando congruencias que el primer caso del teorema de Fermat es cierto para cualquier exponente primo $p < 7000$ (exceptuando el caso $p = 6857$ que no se tomó la molestia de comprobar).
Una interesante pero difícil cuestión es si existen infinitos primos p tal que $2p + 1$ (ó $4p + 1$ ó $8p + 1$ ...) es también primo. Aquí tenemos un resultado dado por Vandiver en 1926:

(2G) *Sean* p, $q = 2kp = 1$, *con* $k \geq 1$, *primos impares. Si* $2k = 2^v p^h$, $h \geq 0$, $p \nmid v$, *y, además, si* 2 *no es una potencia* p*-ésima módulo* q, *entonces el primer caso del teorema de Fermat es cierto para el exponente* p.

Usando (**2B**) , Vandiver dedujo en 1926 el siguiente resultado aunque ya había sido probado por Wendt en 1894 usando su forma del teorema de Sophie Germain:

(2H) *Sean* p, $q = 2kp = 1$, *con* $k \geq 1$, *primos impares, tales que* $2k = 2^v p^h$, $h \geq 0$, $p \nmid v$, *si* $x^p + y^p + z^p \equiv 0 \ (mod\ q)$ *tiene solo la solución trivial, entonces el primer caso del teorema de Fermat es cierto para el exponente* p .

El teorema de Sophie Germain, corolarios y variaciones fueron redescubiertos por varios autores. En 1953, Thébault probó:

(2I) *Si* $m \geq 2$ *es un entero tal que* $2m + 1$ *es primo, si existen enteros no nulos* x, y, z *primos dos a dos tales que* $x^m + y^m = z^m$ *entonces* $2m + 1 \mid xyz$.

Éste resultado fue probado además por Stone en 1963 y por Gandhi en 1966. Gandhi probó en 1965 un resultado similar al de Thébault:

(2J) *Si $m \geq 2$ es un entero tal que $4m+1$ es primo, si existen enteros no nulos x, y, z primos dos a dos tales que $x^m + y^m = z^m$, entonces $4m+1 \mid xyz$.*

Además, en 1969, Perisastri probó:

(2K) *Si $p \geq 51$ es un entero tal que $8p+1$ es primo, si existen enteros no nulos x, y, z primos dos a dos tales que $x^p + y^p = z^p$, entonces $8p+1 \mid xyz$.*

(2L) *Si $m \geq 3$ es un entero tal que $3m+1$ es primo, si existen enteros no nulos x, y, z primos dos a dos tales que $x^m + y^m = z^m$, entonces $3m+1 \mid xyz$.*

Krishnasastri y Perisastri probaron conjuntamente en 1965:

(2M) *Si p es primo es primo impar, x, y, z son enteros tales que $x^m + y^m = z^m$ con $p \nmid xz$, entonces existe un entero $k \geq 1$ tal que $(1+kp) \mid z$.*

Continuando el resultado (**2C**) con el teorema de Sophie Germain tenemos:

(2N) *Sean p y $2p+1$ primos impares, x, y, z son enteros no nulos primos dos a dos tales que $x^p + y^p + z^p = 0$, entonces p^2 divide a uno y solo a uno de los enteros x, y, z.*

Pomey en 1923 y 1925 obtuvo varias condiciones suficientes para el primer caso del teorema de Fermat para el exponente primo p:

(2O) *Sea p primo impar y supongamos que se cumple una de las condiciones:*

1. $p \equiv 1 \ (mod\ 4)$ y $2p+1 \mid 2^p + 1$
2. $p \equiv 3 \ (mod\ 4)$ y $2p+1 \mid 2^p - 1$
3. $4p+1 \mid 2^{2p} + 1$
4. $4p+1 \equiv 5 \ (mod\ 12)$ y $4p+1 \mid 3^{3p} + 1$
5. $8p+1 \mid 2^{4p} - 1$
6. $10p+1 \mid 2^{5p} - 1$

Entonces el primer caso del teorema de Fermat se cumple para el exponente p.

Todos estos resultados no son suficientes para asegurar que existen infinitos exponentes primos p para los cuales se cumple el primer caso del teorema de Fermat. Este resultado fue probado por primera vez en 1897 utilizando la extensión del cuerpo con las raíces p-ésimas de la unidad. Maillet probó que para cada primo impar p, existe un exponente e tal que el primer caso del teorema de Fermat se cumple para el exponente p^e. Esto implica la existencia de un conjunto infinito de exponentes primos 2 a 2 para los cuales

el primer caso era cierto. Esto fue probado por Kapferer en 1964. En 1978, Powell diseñó independientemente una prueba muy simple:

(2P)

1. *Si p es cualquier primo impar, $n = p(p-1)/2 = 2^u m$, donde $u \geq 0$, m impar, si x, y, z son enteros no nulos tales que $x^n + y^n + z^n = 0$ entonces $m.c.d.(m, xyz) \neq 1$.*

2. *Existe un conjunto infinito de exponentes primos dos a dos para los cuales el primer caso del teorema de Fermat es cierto.*

Capítulo 3

El problema local y modular de Fermat

En este capítulo, empezaremos dando un material que nos servirá posteriormente para investigar algunas modificaciones del problema de Fermat original.

3.1. El cuerpo de los números p-ádicos

Para estudiar las propiedades de divisibilidad por un primo p, es conveniente el desarrollo de enteros en base p:

$$a = a_0 + a_1 p + \cdots + a_m p^m,$$

con $0 \leq a_i \leq p-1$, $p^m \leq a \leq p^{m+1}$. Los números así definidos son los enteros p-ádicos. Hensel describió las operaciones suma y producto de enteros p-ádicos y probó un teorema muy importante que tiene que ver con la existencia de enteros p-ádicos que son raíces de ciertos polinomios. Describiremos varios conceptos de los números p-ádicos y los resultados que necesitaremos para la ecuación de Fermat. Sea p primo, a un entero no nulo, sea $v_p(a)$ el exponente de p en la factorización de a como producto de potencias primas de la forma $a = p^{v_p(a)}b$ donde $p \not| b$. Por convenio, se define $v_p(0) = \infty$. Definimos el conjunto

$$\mathbb{Z}_p = \{\frac{a}{b} / a, b \in \mathbb{Z}, b \neq 0, p \not| b, m.c.d(a,b) = 1\} \cup \{0\}$$

Es un subanillo de $\mathbb{Q}$ que contiene a $\mathbb{Z}$. Además, si $r \in \mathbb{Q}$ entonces $v_p(r) \geq 0$ si y solo si $r \in \mathbb{Z}_p$. $\mathbb{Z}_p$ se denomina anillo de valoración de v_p. El único ideal maximal de $\mathbb{Z}_p$ es $\mathbb{Z}_p p = \{\frac{a}{b} \in \mathbb{Z}_p / p|a\}$. El cuerpo $\mathbb{Z}_p/\mathbb{Z}_p p$ es isomorfo a $\mathbb{F}_p$ y se le denomina cuerpo residual de v_p.
La valoración v_p define, en $\mathbb{Q}$, la función d_p como sigue:

Si $a, b \in \mathbb{Q}$, entonces:

$$\begin{cases} d_p(a,b) = p^{-v_p(a-b)} & \text{con } a \neq b, \\ d_p(a,a) = 0 \end{cases}$$

que verifican las siguientes propiedades:

- $d_p(a,b) \geq 0$
- $d_p(a,b) = d_p(b,a)$
- $d_p(a,b) = d_p(a-b,0)$
- $d_p(a+c,b+c) = d_p(a,b)$
- $d_p(a,b) \leq \text{máx}\{d_p(a,c), d_p(b,c)\} \leq d_p(a,c) + d_p(b,c)$

Por tanto, a d_p se le conoce como la distancia p-ádica en $\mathbb{Q}$. La completitud de $\mathbb{Q}$ con la distancia p-ádica es un cuerpo denotado $\hat{\mathbb{Q}}_p$ llamado el cuerpo de los números p-ádicos. Los elementos no nulos α de $\hat{\mathbb{Q}}_p$ se representan:

$$\alpha = \sum_{i=m}^{\infty} a_i p^i$$

con $0 \leq a_i \leq p-1$, $m \in \mathbb{Z}$, $a_m \neq 0$
Por tanto, la valoración $\hat{v}_p$ del cuerpo $\hat{\mathbb{Q}}_p$ definida por

$$\hat{v}_p\left(\sum_{i=m}^{\infty} a_i p^i\right) = m$$

toma valores enteros o infinito.

3.2. Polinomios con coeficientes p-ádicos

Si $f(x) = a_0 x^n + a_1 x^{n-1} + \cdots + a_n \in \hat{\mathbb{Q}}_p[x]$, definimos $\tilde{v}_p(f) = \text{mín}_{0 \leq i \leq n}\{v_p(a_i)\}$. Si $f, g \in \hat{\mathbb{Q}}_p[x]$, con $g \neq 0$, definimos

$$\tilde{v}_p\left(\frac{f}{g}\right) = \tilde{v}_p(f) - \tilde{v}_p(g),$$

lo cual esta bien definido. Entonces $\tilde{v}_p$ es una valoración del cuerpo $\hat{\mathbb{Q}}_p$, cuya restricción a $\mathbb{Q}_p$ es la valoración v_p. Por simplificar, escribiremos v_p en vez de $\tilde{v}_p$.
Si $f, g \in \hat{\mathbb{Q}}_p[x]$, escribimos $f \equiv g \ (mod\ p^n)$ cuando $v_p(f-g) \geq n$ o lo que es lo mismo, p^n divide a cada coeficiente de $f-g$. Para cada $f = \sum_{i=0}^{m} a_i x^i \in \hat{\mathbb{Z}}_p[x]$, donde $\hat{\mathbb{Z}}_p$ es la clausura topológica de $\mathbb{Z}_p$ en $\hat{\mathbb{Q}}_p$, denotamos $\overline{f} = f \ (mod\ p)$ al polinomio $\sum_{i=0}^{m} \overline{a_i} x^i \in \mathbb{F}_p[x]$

Ahora daremos algunos resultados conocidos sobre polinomios en $\hat{\mathbb{Q}}_p[x]$. El polinomio $f \in \hat{\mathbb{Z}}_p[x]$ se dice primitivo cuando $v_p(f) = 0$. Cada polinomio $f \in \mathbb{Z}_p[x]$ puede ser escrito como $f = af_1$ donde $a \in \mathbb{Z}$ y $f_1 \in \hat{\mathbb{Z}}_p[x]$ y f_1 es primitivo.

***(3A) Lema de Gauss**. Si $f, g \in \hat{\mathbb{Z}}_p[x]$ son polinomios primitivos, entonces $f \cdot g$ es tambien un polinomio primitivo.*

***(3B)** Si $f \in \mathbb{Z}_p[x]$ es primitivo y $f = g \cdot f$ con $g, h \in \hat{\mathbb{Q}}_p[x]$, entonces $f = f_1 \cdot g_1$ para algunos polinomios primitivos $f_1, g_1 \in \mathbb{Z}_p[x]$, tales que $deg(g_1) = deg(g)$, $deg(h_1) = deg(h)$.*

***(3C)** Si $f \in \hat{\mathbb{Z}}_p[x]$, entonces f es irreducible en $\hat{\mathbb{Z}}_p[x]$ si y solo si es irreducible en $\hat{\mathbb{Q}}_p[x]$.*

***(3D)** Si $f \in \hat{\mathbb{Z}}_p[x]$ es no constante y primitivo, y si f no divide al polinomio no constante $g \in \hat{\mathbb{Z}}_p[x]$, entonces f y g son primos relativos, es decir, si $\exists h \in \mathbb{Z}_p[x]$ tal que h divide a f y g, y $deg(h) = 0$.*

***(3E)** Si $f, g \in \hat{\mathbb{Z}}_p[x]$ son no constantes y primos relativos, entonces existen polinomios $s, t \in \hat{\mathbb{Z}}_p[x]$ tales que $s \cdot f + t \cdot g$ es un elemento no nulo de $\hat{\mathbb{Z}}_p[x]$.*

***(3F)** Si $f, g, h \in \hat{\mathbb{Z}}_p[x]$, siendo f irreducible y f divide a $g \cdot h$ entonces f divide a g o f divide a h.*

***(3G)** Si $g, h \in \hat{\mathbb{Z}}_p[x]$ son no constantes y primos relativos, si g o h es primitivo y ambos g y h dividen a f, entonces $g \cdot h$ divide a f.*

***(3H)** Cada polinomio no nulo $f \in \hat{\mathbb{Z}}_p[x]$ puede ser escrito como un producto $F = ag_1 \cdots g_m$ donde $a \in \hat{\mathbb{Z}}_p[x]$, y $g_1, \ldots, g_m \in \hat{\mathbb{Z}}_p[x]$ son polinomios irreducibles con $m \geq 0$. Además, a y $g_1, \ldots, g_m$ están definidos por una unidad en $\hat{\mathbb{Z}}_p[x]$.*

***(3I)** Sean $f, g \in \hat{\mathbb{Z}}_p[x]$ polinomios no constantes. Entonces las siguientes condiciones son equivalentes:*

1. *Existe un polinomio no constante $h \in \hat{\mathbb{Z}}_p[x]$ que divide tanto a f como a g.*
2. *Existen unos polinomios no nulos $f_1, g_1 \in \hat{\mathbb{Z}}_p[x]$ tales que $deg(f_1) < deg(f)$, $deg(g_1) < deg(g)$, y se cumple $g_1 \cdot f + f_1 \cdot g = 0$.*

Ahora vamos a considerar la resultante y el discriminante de polinomios en $\hat{\mathbb{Z}}_p[x]$.

***(3J)** Para que $f = \sum_{i=0}^{m} a_i x^{m-i}$ y $g = \sum_{j=0}^{n} b_j x^{n-j}$ (donde $m, n > 0 y f, g \in \hat{\mathbb{Z}}_p[x]$) tengan un factor común no constante, es necesario y suficiente que $R(f, g) = 0$.* Se define la resultante, $R(f, g)$, como el determinante de la siguiente matriz:

$$\begin{pmatrix} a_0 & a_1 & \cdots & \cdots & a_m & 0 & 0 \\ 0 & a_0 & a_1 & \cdots & \cdots & a_m & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & a_0 & a_1 & \cdots & \cdots & a_m \\ 0 & 0 & b_0 & b_1 & \cdots & \cdots & b_n \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & b_0 & b_1 & \cdots & \cdots & b_n & 0 \\ b_0 & b_1 & \cdots & \cdots & b_n & 0 & 0 \end{pmatrix}$$

(3K) *Sean $f, g \in \hat{\mathbb{Z}}_p[x]$ polinomios primos relativos no constantes tales que $v_p(R(f,g)) = \rho$. Entonces cada polinomio no nulo $h \in \hat{\mathbb{Z}}_p[x]$ tal que $v_p(h) \geq \rho$ y $deg(h) < deg(f) + deg(g)$ puede ser escrito de forma única como $h = g_1 \cdot f + f_1 \cdot g$ donde $f_1, g_1 \in \hat{\mathbb{Z}}_p[x]$, $v_p(f_1) \geq v_p(h) - \rho$, $v_p(g_1) \geq v_p(h) - \rho$, $deg(f_1) < deg(f)$ y $deg(g_1) < deg(g)$.*

(3L) *Sea $g \in \hat{\mathbb{Z}}_p[x]$ un polinomio no constante. Para que exista un polinomio no constante $g \in \hat{\mathbb{Z}}_p[x]$ tal que g^2 divida a f, es necesario y suficiente que $Discr(f) = 0$.* Se define el discriminante $Discr(f) = R\left(f, \dfrac{\partial f}{\partial x}\right)$.

Ahora investigaremos el comportamiento del resultante $R(f,g)$ cuando f, g son polinomios suficientemente cercanos, en relación a la métrica definida por la valoración v_p en $\hat{\mathbb{Q}}_p(x)$.

(3M) *Si $f, g, f_1, g_1 \in \hat{\mathbb{Z}}_p[x]$ son polinomios no constantes y $v_p(f_1 - f) \geq \alpha$, $v_p(g_1 - g) \geq \beta$, entonces $v_p(R(f_1, g_1) - R(f,g)) \geq min\{a, b\}$.*

(3N) *Con la notación anterior, si $f, f_1 \in \hat{\mathbb{Z}}_p[x]$ son polinomios no constantes y $v_p(f_1 - f) \geq \alpha$, entonces $v_p(Discr(f) - Discr(f_1)) \geq \alpha$.*

(3O) *Si $f, g \in \hat{\mathbb{Z}}_p[x]$, $\overline{f} = f \ (mod\ p)$, $\overline{g} = g \ (mod\ p)$, entonces $R(\overline{f}, \overline{g}) = \overline{R(f,g)}$ y $Discr(\overline{f}) = \overline{Discr(f)}$.*

Decimos que los polinomios no constantes $f, g \in \hat{\mathbb{Z}}_p[x]$ son primos relativos módulo p cuando $\overline{f}, \overline{g}$ son primos relativos en $\mathbb{F}_p$. De la misma manera, se dice que f es irreducible módulo p si $\overline{f}$ es un polinomio irreducible en $\mathbb{F}_p$. Con estas definiciones, tenemos:

(3P) *$f, g \in \hat{\mathbb{Z}}_p[x]$ son primos relativos módulo p si y solo si el resultante es una unidad en $\hat{\mathbb{Z}}_p[x]$, es decir, si y solo si $v_p(R(f,g)) = 0$.*

(3Q) *Sean $f, g \in \hat{\mathbb{Z}}_p[x]$ polinomios irreducibles módulo p. Entonces p divide a $R(f,g)$ si y solo si $f \equiv g \ (mod\ p)$.*

(3R) *Si $f \in \hat{\mathbb{Z}}_p[x]$ es irreducible módulo p, entonces p no divide a $Discr(f)$.*

(3S) *Sea $f \in \hat{\mathbb{Z}}_p[x]$ tal que $\overline{f}$ no es constante. Entonces f tiene un factor irreducible múltiple módulo p si y solo si p divide a $Discr(f)$.*

3.3. El lema de Hensel

Este es un resultado muy importante, probado por Hensel en 1908, que afirma la existencia, bajo condiciones adecuadas, de raices p-ádicas de polinomios. Aquí enunciamos el lema de Hensel:

(3T) *Sea $F, g, h \in \hat{\mathbb{Z}}_p[x]$ tales que:*

1. *$deg(g) = m > 0$, $deg(h) = n > 0$, $deg(F) = m + n$, g es mónico y $deg(F - gh) < deg(F)$;*
2. *$v_p(R(f, g)) = \rho \geq 0$; y*
3. *$v_p(F - gh) = \alpha > 2p$*

Entonces existen $G, H \in \hat{\mathbb{Z}}_p[x]$ tales que $v_p(G - g) \geq \alpha - \rho$, $v_p(H - h) \geq \alpha - \rho$, $deg(G) = deg(g)$, $deg(H) = deg(h)$, G es mónico, H, h tienen los mismos coeficientes líderes y, finalmente, $F = G \cdot H$.

Ahora vamos a enunciar el lema de Hensel en su forma mas habitual:

(3U) *Sea $F, g, h \in \hat{\mathbb{Z}}_p[x]$ tales que:*

1. *$deg(g) = m > 0$, $deg(h) = n > 0$, $deg(F) = m + n$, g es mónico y $deg(F - gh) < deg(F)$;*
2. *g, h son primos relativos módulo p; y*
3. *$F \equiv g \cdot h \ (mod\ p)$.*

Entonces existen $G, H \in \hat{\mathbb{Z}}_p[x]$ tales que $G \equiv g \ (mod\ p)$, $H \equiv h \ (mod\ p)$, $deg(G) = deg(g)$, $deg(H) = deg(h)$, G es mónico, H, h tienen los mismos coeficientes líderes y, finalmente, $F = G \cdot H$.

Otra forma muy común del lema de Hensel es:

(3V) *Sea $F \in \hat{\mathbb{Z}}_p[x]$ con $deg(F) \geq 1$, sea $a \in \hat{\mathbb{Z}}_p[x]$ una raíz simple de $F(x) \equiv 0 \ (mod\ p)$. Entonces existe un $b \in \hat{\mathbb{Z}}_p[x]$ tal que $\overline{b} = \overline{a}$ y $F(b) = 0$.*

3.4. Problema local y modular de Fermat

Nuestro objetivo es probar que para cada primo q, la ecuación de Fermat tiene solución en los enteros q-ádicos. Nuestra herramienta será el lema de Hensel.

(3W) *Para cada primo q y cada primo p, la ecuación $x^p + y^p = z^p$ tiene solución no trivial en los enteros q-ádicos.*

(3X) *Sea $n \geq 1$ y sea p un primo impar. Las siguientes condiciones son equivalentes:*

1. *Existen enteros x, y, z no múltiplos de p tales que $x^{p^n} + y^{p^n} + z^{p^n} \equiv 0 \ (mod\ p^{n+1})$.*
2. *Para cada $m \geq 0$ existen enteros x_m, y_m, z_m no múltiplos de p tales que $x_m^{p^n} + y_m^{p^n} + z_m^{p^n} \equiv 0 \ (mod\ p^{n+1+m})$ y $x_{m+1} \equiv x_m \ (mod\ p^{m+1})$, $y_{m+1} \equiv y_m \ (mod\ p^{m+1})$, $z_{m+1} \equiv z_m \ (mod\ p^{m+1})$.*

(3Y) *Sea p un primo impar. Las siguientes condiciones son equivalentes:*

1. *Existen unidades α, β, γ de $\hat{\mathbb{Z}}_p$ tales que $\alpha^p + \beta^p + \gamma^p = 0$.*
2. *Existen enteros x_0, y_0, z_0 no múltiplos de p, tal que $x_0^p + y_0^p + z_0^p \equiv 0 \ (mod\ p^2)$.*
3. *Para cada $n \geq 0$ existen enteros x_n, y_n, z_n no multiplos de p, tal que $x_n^p + y_n^p + z_n^p \equiv 0 \ (mod\ p^{n+2})$ y $x_{n+1} \equiv x_n \ (mod\ p^{n+1})$, $y_{n+1} \equiv y_n \ (mod\ p^{n+1})$, $z_{n+1} \equiv z_n \ (mod\ p^{n+1})$.*

Además las condiciones de (3Y) son equivalentes a:

- Existen enteros x, y no múltiplos de p, y una unidad $\gamma \in \hat{\mathbb{Z}}_p$ tal que $x^p + y^p + \gamma^p = 0$.

De la misma forma tenemos:

(3Z) *Sean q, p primos distintos. Las siguientes condiciones son equivalentes:*

1. *Existen unidades α, β, γ de $\hat{\mathbb{Z}}_p$ tales que $\alpha^p + \beta^p + \gamma^p = 0$.*
2. *Existen enteros x_0, y_0, z_0 no múltiplos de q, tal que $x_0^p + y_0^p + z_0^p \equiv 0 \ (mod\ q)$.*
3. *Para cada $n \geq 0$ existen enteros x_n, y_n, z_n no multiplos de q, tal que $x_n^p + y_n^p + z_n^p \equiv 0 \ (mod\ q^{n+1})$ y $x_{n+1} \equiv x_n \ (mod\ q^{n+1})$, $y_{n+1} \equiv y_n \ (mod\ q^{n+1})$, $z_{n+1} \equiv z_n \ (mod\ q^{n+1})$.*

Como en el enunciado anterior, las condiciones de (3Z) son equivalentes a:

- Existen enteros x, y no múltiplos de q, y una unidad $\gamma \in \hat{\mathbb{Z}}_p$ tal que $x^p + y^p + \gamma^p = 0$.

Ahora estudiaremos la crongruencia:

$$x^n + y^n + z^n \equiv 0 \ (mod\ q),$$

donde q es un primo impar, $n \geq 0$ y q no divide a n. Sea $N(n,q) = \#\{(x,y,z) \,|\, 1 \leq x,y,z < q,\ x^n+y^n+z^n \equiv 0 \ (mod\ q)\}$. Por último, damos el siguiente enunciado probado por Libri en 1832 y ,posteriormente, por Pepin en 1880, Pellet en 1887 y Matthews en 1895.

(3A') *Sea p un número primo. Si existen infinitos primos q tales que $N(p,q) = 0$, entonces el último teorema de Fermat es cierto para el exponente p.*

Capítulo 4

El teorema de Fermat

Vamos a exponer el razonamiento para demostrar el teorema de Fermat. Suponemos que existen un número natural $n \geq 3$ y unos enteros positivos a, b, c tales que $a^n + b^n = c^n$. La prueba se realiza por reducción al absurdo. No se encontraron contradicciones con los resultados en teoria de numeros elementales, ni con resultados sobre cuerpos numéricos, ni con otros resultados hasta que el teorema de Fermat se expresó en terminos de curvas elípticas. La prueba del teorema de Fermat se estableció de la siguiente forma:

1. Asociar una curva elíptica a una hipotética solucion no trivial de la ecuación de Fermat con un exponente arbitrario $n \geq 5$.
2. Obtener una contradicción asumiendo la validez de una cierta conjetura sobre curvas elípticas y formas modulares.
3. Probar la validez de la conjetura.

Estos pasos requieren conceptos muy sofisticados y una teoría profunda. Las nociones clave que se necesitan para poder entender la prueba son curvas elípticas, formas modulares y representaciones de Galois.

4.1. Las curvas de Frey

Para A, B enteros positivos primos entre si, con A divisible por 16, Frey consideró la curva elíptica, a la que denotaremos E, de ecuación

$$y^2 = x(x - A)(x + B) \tag{4.1}$$

y estudió sus propiedades.
Si el teorema de Fermat es falso para el exponente primo $q \geq 5$, sean a, b, c enteros positivos primos entre si, con a par, tal que $a^q + b^q = c^q$. Sea $A = a^q$, $B = b^q$. La curva de Frey asociada presenta propiedades diferentes a las de otras curvas elípticas. Frey se

convenció de que tal situación no era posible y se imaginó un metodo para derivar una contradicción con la conjetura de Simura-Taniyama.
Aquí tenemos algunas propiedades de las curvas de Frey: el discriminante mínimo de la curva de Frey es

$$\Delta = \frac{a^{2q}b^{2q}(a^q + b^q)^2}{2^8} = \frac{(abc)^{2q}}{2^8}$$

Como $\Delta \neq 0$, la curva es no singular, por lo tanto es una curva elíptica.
Para cada primo p que no divida a Δ, tomamos la congruencia

$$y^2 \equiv x(x - a^q)(x + b^q) \pmod{p}, \tag{4.2}$$

que define una curva en el espacio bidimensional sobre el cuerpo finito $\mathbb{F}_p$. Ya que p no divide a Δ, la curva es no singular, luego es una curva elíptica. Por otro lado, si p divide a Δ, la curva es singular. El tipo de singularidades está codificado en el invariante llamado el *conductor*. Definimos el conductor como el producto de primos en el que E tiene una mala reducción, lo cual no es más que el conjunto de primos que divide el discriminante mínimo. Los primos p que dividen al conductor son exactamente los mismos que dividen al invariante, que son los primos p para los cuales la curva en $\mathbb{F}_p \times \mathbb{F}_p$ tiene singularidad. En este caso, el conductor N es libre de cuadrados, luego es de la forma

$$N = \prod_{p|\Delta} p$$

Las curvas elípticas con conductor libre de cuadrado se denominan *semiestables*. Por tanto, las curvas de Frey son semiestables. Es sabido que, si el teorema de Fermat se supone falso para un exponente primo q, entonces q debe ser muy grande; además, como la ecuación de Fermat es homogénea, el discriminante es una potencia, y esto difícilmente puede ser posible.
Contamos el numero de puntos de la curva de Frey módulo p (para cada p que no divide a Δ). A esto añadimos 1 más, que corresponde al punto en el infinito en el plano proyectivo asociado. Sea ν_p el número de puntos y $a_p = p + 1 + \nu_p$ donde a_p no tiene por qué ser estrictamente positivo. La regla para determinar estos enteros a_p utiliza formas modulares.

4.2. Formas modulares

Sea $N \geq 1$ entero. Sea $\Gamma_0(N)$ el conjunto de todas las matrices 2×2

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

donde a, b, c, d son enteros, N divide a c y $ad - bc = 1$. $\Gamma_0(N)$ es un grupo multiplicativo llamado el *grupo de congruencia de nivel* N. Denotemos H como el semiplano superior, que es, $H = \{z = x + iy \in \mathbb{C} | y > 0\}$. $\Gamma_0(N)$ actúa sobre H de la siguiente forma:

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} z = \frac{az+b}{cz+d}$$

Asociados al grupo $\Gamma_0(N)$ hay puntos llamados *cúspides*; que son puntos en el infinito de la semirrecta $\{iy | y \geq 0\}$ y otros puntos en $H \cup \mathbb{Q}$ (cuando $N > 1$).
Una forma modular de nivel N (y peso 2, que son las únicas que vamos a considerar) es una función f que va de $H^* = H \cup \{\text{cúspides de } \Gamma_0(N)\}$ a $\mathbb{C}$ tal que:

1. Para todo $\begin{pmatrix} a & d \\ c & d \end{pmatrix} \in \Gamma_0(N)$ y $z \in H^*$:

$$f\left(\frac{az+b}{cz+d}\right) = (cz+d)^2 f(z);$$

2. f es holomorfa en cada punto de H^* (requiere una definición apropiada en las cúspides).

Una forma modular que se hace cero en todas las cúspides se llama una forma parabólica.

La teoría de formas modulares es muy rica. Aquí enunciaremos algunos datos relevantes:

1. El conjunto $M_2(N)$ de formas modulares de nivel N y peso 2 es un espacio vectorial de dimensión finita sobre $\mathbb{C}$ y el subconjunto de formas parabólicas es un subespacio. Para el nivel $N = 2$ el subespacaio de las formas parabólicas consiste solo en el 0.

2. Hay un producto escalar en $M_2(N)$, así que es posible considerar la ortogonalidad en $M_2(N)$.

3. Sea $N \geq 1$. Si m divide a N entonces $M_2(M) \subseteq M_2(N)$. También existe la inclusión de $M_2(M)$ en $M_2(N)$ definido de la siguiente manera: si $f \in M_2(N)$ sea $\tilde{f}(z) = f((N/M)z)$ para cada $z \in H^*$; entonces $\tilde{f} \in M_2(N)$

4. Una forma $f \in M_2(N)$ se llama *forma vieja* si f está en el subespacio de $M_2(N)$ generado por las imagenes de las funciones consideradas en el apartado anterior, para todo m dividiendo a N. Una forma $f \in M_2(N)$ se llama *forma nueva* si esta en el subespacio ortogonal al subespacio de formas viejas.

5. Como
$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_0(N)$$
entonces $f(z+1) = f(z)$ para cada forma modular y para cada z. Por tanto, f tiene un desarrollo de Fourier, de la forma
$$f(z) = \sum_{n=0}^{\infty} c_n e^{2\pi i n z}. \tag{4.3}$$
Para formas parabólicas, $c_0 = 0$.

6. Hecke definió para cada $n \geq 1$ coprimo con el nivel N, un operador lineal $T(n)$ de $M_2(N)$. Una forma modular que es un autovalor para todos los operadores de Hecke $T(n)$ se llama una *autoforma*, o *forma propia*. Todo esto, aparte de mas operadores asociados a los enteros, generan el álgebra de Hecke, cuyas propiedades son de esencial importancia.

Ahora vamos a hablar de la relacion entre curvas elípticas y formas modulares. Para una curva elíptica dada, los números a_p contienen una información muy importante de la curva de manera local. Es crucial relacionar esos datos locales por medio de algún invariante global.
Esta idea es una modificación del hecho de que todo numero natural es producto de potencias de primos de forma única. Euler ya introdujo esta relación:

$$\prod_p \left(1 - \frac{1}{p^s}\right)^{-1} = \sum_{n=1}^{\infty} \frac{1}{n^s}.$$

Primero se tomo $s > 1$ como un número real, para el cuál ambos lados convergen y son iguales. Riemann tuvo la idea de permitir que s fuese un número complejo con $Re(s) > 1$. La función superior, por tanto, se conoce como la función zeta de Riemann, donde para probar su convergencia se usaron L-series.
En una gran analogía con los cuerpos numéricos, las curvas elípticas también presentan propiedades analíticas muy importantes. Los números a_p para cada primo p definidos anteriormente se combinan multiplicativamente para definir unos a_n, con n natural, para asi crear unas series de Dirichlet, llamadas las L-series de la curva elíptica, que convergen para $Re(s) > \frac{3}{2}$.
También se ha observado que en ciertas curvas elípticas los números a_p coinciden con los coeficientes c_p del desarrollo en series de Fourier de alguna forma modular. Las curvas elípticas con esta propiedad se denominan curvas elípticas modulares.
En 1955, Taniyama propuso unos problemas sobre la cuestión anterior, si la conjetura de Hasse fuese cierta, ¿se asociarían L-series con alguna función automorfa o incluso a alguna forma modular?
En 1964, Shimura enunció una conjetura muy específica sobre la modularidad de curvas elípticas, también trabajada por Taniyama y, en menor parte, por Weil. A esta conjetura se la conoció posteriormente bajo el nombre de la conjetura de Shimura-Taniyama.

4.3. La conjetura de Shimura-Taniyama

Teorema 5 (Shimura-Taniyama) *Toda curva elíptica es modular.*

La conjetura de Shimura-Taniyama dice que toda curva elíptica es modular. Esto es una forma breve de expresar lo siguiente:

Si E es cualquier curva elíptica definida sobre $\mathbb{Q}$, y si N es su conductor, entonces hay una nueva autoforma parabólica f de nivel N, cuyos coeficientes de Fourier c_n son enteros tales que para todo primo p que no divide a N, $c_p = a_p$, donde a_p se define contando el numero de puntos de E en $\mathbb{F}_p$.

Explicamos como es posible asociar una curva elíptica. Sea $z_0 \in H$. Para cada $\gamma \in \Gamma_0(N)$ consideramos

$$w_{z_0}(\gamma) = \int_{z_0}^{\gamma(z_0)} f(z)dz;$$

que es independiente del camino. El conjunto $\{w_{z_0}(\gamma)|\gamma \in \Gamma_0(N)\}$ es independiente de z_0, así que depende únicamente de f. Teniendo en cuenta que los coeficientes de Fourier de f son enteros, el conjunto definido es un mallado en H, que es el conjunto de todas las combinaciones lineales, con los coeficientes enteros, de dos numeros en H^*. Este mallado da lugar de la manera habitual a un toro analítico, por lo tanto a una curva elíptica E que tiene una ecuación con coeficientes en $\mathbb{Z}$ (así E se define sobre $\mathbb{Q}$). Sea $C_2(N) = \{f \in M_2(N)|f$ es una autoforma cuspidal cuyos coeficientes de Fourier son enteros$\}$. Esta construcción asocia a cada $f \in C_2(N)$ una curva elíptica E definida sobre $\mathbb{Q}$. Además, el conductor de E es de nivel N de f y para cada primo p que no divide al discriminante de E, los coeficientes de Fourier c_p de f son iguales a los numeros a_p.

Por último daremos una modificación necesaria de la conjetura de Shimura-Taniyama para la prueba del último teorema de Fermat:

Teorema 6 *Toda curva elíptica semiestable con coeficientes racionales es modular.*

La prueba es muy técnica pero la idea es relativamente simple. Suponemos que E es una curva elíptica semiestable con conductor N. Tenemos que probar que E es modular. Sabemos que podemos construir una representacion de Galois

$$\rho(E, p^\infty) : G \mapsto GL_2(\mathbb{Z}_p)$$

asociada a la curva E para cualquier primo p, donde G es un grupo de Galois de $\overline{\mathbb{Q}}|\mathbb{Q}$ y $\overline{\mathbb{Q}}$ representa el cuerpo de los numeros algebraicos. Para probar que E es modular, debemos mostrar que esta representación es modular. La prueba de que $\rho(E, p^\infty)$ es modular involucra la búsqueda de una autoforma f en $S(N)$ con propiedades adecuadas. Las propiedades requeridas son que los autovalores de f, los cuales son sus coeficientes en la serie de Fourier, deben ser congruentes módulo q con la traza $(\rho(E, p^\infty)(\sigma_p))$ para todos excepto un número finito de primos q ($\sigma_q \in G$ se conoce como el elemento de Frobenius). Se sabe que la traza es, para el primo q hasta pN, el coeficiente $a_p = q + 1 - \#(E(\mathbb{F}_q))$ de la L-serie $L(E, s)$.

La parte mas extensa y dura del trabajo de Wiles fue probar un resultado general que aproximadamente dice que si $\rho(E, p)$ es modular, entonces tambien lo es $\rho(E, p^\infty)$. En otras palabras, para probar que E es modular, en realidad es suficiente probar que

$$\rho(E, p) : G \mapsto GL_2(\mathbb{Z}/\mathbb{Z}_p)$$

es modular. Este es el llamado "problema de elevación modular".

El problema se reduce a asumir que $\rho(E, p)$ es modular e intentar elevar la representación a $\rho(E, p^\infty)$. Esto se puede hacer principalmente trabajando con la teoría de representaciones tanto como sea posible, sin referencias específicas a la curva E. La prueba usa un concepto llamado "deformación", que sugiere intuitivamente qué va pasando en el proceso de elevación.

4.4. El trabajo de Ribet y Wiles

Antes de seguir, vamos a recordar unas definiciones que nos harán falta:

Definición 7 *Se define el conductor como un producto de primos en el que E tiene una mala reducción, es decir, el conjunto de primos que divide el discriminante mínimo.*

Definición 8 *Se define una autoforma, o forma propia como una forma modular que es un autovalor para todos los operadores de Hecke T_n.*

Definición 9 *Se define forma parabólica como una forma modular que se hace cero en todas las cúspides.*

Antes de que Frey prestara atención a la inusual curva elíptica que resultaría si hubiera una solución no trivial de la ecuación de Fermat, Jean-Pierre Serre formuló varias conjeturas que, a veces solas y a veces junto con la conjetura de Shimura-Taniyama, pudieron son útiles para probar el último teorema de Fermat.

Kenneth Ribet rápidamente encontró una manera para probar una de estas conjeturas:

Teorema 10 *Si hay una solución (x, y, z, n) de la ecuación de Fermat, entonces la curva elíptica definida por la ecuación*

$$y^2 = x(x - A)(x + B)$$

donde A y B se definen como en la curva de Frey, es semiestable pero no modular.

La conjetura en sí misma no hablaba acerca de las curvas de Frey ni del úlltimo teorema de Fermat. En vez de eso, simplemente establecía que si la representacion de Galois asociada con una curva elíptica E tiene ciertas propiedades, entonces E no puede ser modular. Específicamente, no puede ser modular en el sentido de que existe una forma modular que lleva a la misma representación de Galois.

Necesitamos introducir un poco de notación adicional para explicarlo mejor. Sea $S(N)$ el espacio vectorial de formas parabólicas de $\Gamma_0(N)$ de peso 2. La teoría clásica de formas modulares muestra que $S(N)$ puede ser identificado con el espacio de diferenciales holomórficas sobre una cierta superficie de Riemann $X_0(N)$. Además, la dimensión de

$S(N)$ es finita e igual al género de $X_0(N)$. El género es una propiedad topológica de superficies que corresponde al número de huecos de una superficie (por ejemplo, un toro tiene género 1). Pero hay fórmulas mas explícitas para el género de $X_0(N)$. Estas fórmulas involucran el índice de $\Gamma_0(N)$. Un hecho de crucial importancia es que para $N < 11$, el género de $X_0(N)$, y por tanto la dimensión de $S(N)$, es cero. En otras palabras, $S(N)$ solo contiene la forma constante 0 en ese caso. Usaremos este hecho acerca de $S(2)$ pronto.

Como ya vimos antes, hay ciertos operadores $T(n)$ llamados operadores de Hecke sobre espacios de formas modulares y para el subespacio $S(N)$ en particular, ya que éstos preservan el peso de una forma. Todos los $T(n)$ son operadores lineales sobre $S(N)$. Recordamos que si hay una forma parabólica f en $S(N)$ que es simultáneamente un autovector de todo $T(n)$, f es una autoforma. La autoforma f se dice normalizable si su coeficiente principal en un desarrollo de Fourier es 1. En este caso, los autovalores $\lambda(n)$ se vuelven los coeficientes de la expansión en serie de Fourier.

$$f(z) = \sum_{n=0}^{\infty} c_n e^{2\pi i n z}.$$

Se puede probar que si $f(z)$ es una forma parabólica, entonces existe una descomposición para la L-función $L(f, s)$. Esto es de gran ayuda para relacionar L-funciones de formas y L-funciones de curvas elípticas.

Si $f \in S(N)$ es una autoforma normalizada de todos los operadores de Hecke, se puede demostrar que los coeficientes en la expansión de Fourier son todos los números algebraicos y que ellos generan una extensión finita K de $\mathbb{Q}$. Los ideales primos del anillo de enteros K son análogos de los primos en $\mathbb{Q}$. En el caso de que f sea una autoforma normalizada, es posible la construcción de la representacion de Galois $\rho(f, p)$ de $Gal(\overline{\mathbb{Q}}/\mathbb{Q})$ para cualquier ideal primo p del anillo de enteros K.

Al fin prodemos describir lo que Ribet probó. Supongamos que E es una curva elíptica semiestable con conductor N y que su representación de Galois asociada $\rho(f, p)$ para algún primo p tiene ciertas propiedades. Supongamos que 2 divide a N (lo cual es cierto para las curvas de Frey). Si E es modular, entonces hay una autoforma normalizada f y un ideal primo p tal que la representación de Galois $\rho(f, p)$ es $\rho(E, p)$. Ribet mostró que es posible encontrar un primo impar $q \neq p$ el cual divide a N tal que hay otra $f_1 \in S(N/q)$ y un ideal primo correspondiente p_1 del anillo de los enteros en el cuerpo generado por los coeficientes de f_1 tal que $\rho(f_1, p_1)$ de esencialmente la misma representación de Galois. Esta es conocida como la conjetura del "descenso de nivel"puesto que afirma que bajo las condiciones adecuadas hay una autoforma de un nivel mas bajo que da esencialmente la misma representación de Galois.

Este proceso puede ser repetido tanto como N tenga factores primos impares. Es im-

portante que la curva E sea semiestable para que asi N sea libre de cuadrados. Esto dice que los factores primos impares de N pueden ser eliminados, así que debe haber una autoforma no trivial de nivel 2, es decir, en $S(2)$ esto da la misma representacion de Galois. Y esto es una contradicción, ya que como vimos anteriormente $S(2)$ tiene dimensión 0, por tanto no contiene autoformas no triviales. Esto entra en contradicción con la conjetura de Shimura-Taniyama.

Bibliografía

[1] Cassels, J.W.S.: *Lectures on Elliptic Curves.* Cambridge University Press, Cambridge, 1991.

[2] Germain, S.: *Letter to Gauss.* Nov. 21,1804; reimpreso en *Oeuvres Philosophiques.* (editados por H. Stupuy), Ritti, Paris, 1879.

[3] Koblitz, N.: *Introduction to Elliptic Curves and Modular Forms.* Springer-Verlag, New York, 1984.

[4] Legendre, A.M.: *Théorie des Nombres.* (3^e édition), Vol. II, p. 5, Firmin Didot Frères, Paris, 1830; reimpreso por A. Blanchard, Paris, 1955.

[5] Nagell, T.: *Introduction to Number Theory.* Wiley, New York, 1951; reimpreso por Chelsea, New York, 1962.

[6] Ribenboim, P.: *Fermat's Last Theorem for Amateurs.* Springer-Verlag, New York, 1999.

[7] Ribet, K.A.: *From the Taniyama-Shimura conjecture to Fermat's last theorem.* Ann. Fac. Sci. Toulouse Math., (5), 11 (1990), no. 1, 116-139.

[8] Tate,J. y Silverman, J.H.: *Rational Points on Elliptic Curves.* Springer-Verlag, New York, 1992.

[9] Taylor, R. y Wiles, A.: *Ring theoretic properties of certain Hecke algebras.* Ann. of Math., (2), 141 (1995), 553-572.

[10] Wiles, A.: *Modular elliptic curves and Fermat's last theorem.* Ann. of Math., (2), 141 (1995), 443-551.

[11] https://tecdigital.tec.ac.cr/revistamatematica/ContribucionesV4n3/Fermat/index.html