ARITMETICA Y GEOMETRIA

(CURSO B3)

Dr. Ricardo Baeza
(U. DE CHILE)

ARITMETICA Y GEOMETRIA

R. BAEZA[1]

El propósito de estas tres charlas es explicar a través de un ejemplo algunas interrelaciones que existen entre aritmética (teoría de números) geometría (geometría algebraica) y el análisis. No pretendemos dar demostraciones de los resultados expuestos aquí, sino que pondremos énfasis en las relaciones que existen entre ellos.

Denotaremos por $\mathbb{Z}$ el anillo de enteros racionales y por $\mathbb{Q}$ los números racionales. $\mathbb{R}$ denotará el cuerpo de los números reales y $\mathbb{C}$ de los números complejos.

Uno de los problemas básicos de la aritmética es el siguiente:

Sea $f(x_1,\ldots,x_n) \in \mathbb{Z}[x_1,\ldots,x_n]$ un polinomio con coeficientes enteros, es decir

$$f(x_1,\ldots,x_n) = \sum a_{i_1\ldots i_n} x_1^{i_1}\ldots x_n^{i_n}$$

1) FACULTAD DE CIENCIAS. UNIVERSIDAD DE CHILE.

con $a_{i_1 \ldots i_n} \in \mathbb{Z}$ (o también en $\mathbb{Q}$ más general). El problema es encontrar todos los tuplos $(a_1,\ldots,a_n) \in \mathbb{Z}x\ldots x\mathbb{Z}$ tal que

(1) $\quad f(a_1,\ldots,a_n) = 0$

O más general, todos los tuplos de números racionales $(a_1,\ldots,a_n) \in \mathbb{Q}x\ldots x\mathbb{Q}$ que satisfacen (1). Si $(a_1,\ldots,a_n) \in \mathbb{Z}^n$ satisface (1), se llama solución entera de la ecuación $f(X_1,\ldots,X_n) = 0$; si $(a_1,\ldots,a_n) \in \mathbb{Q}^n$, se llama solución racional. Una ecuación de este tipo se llama **ecuación Diofántica**. Encontrar todas las soluciones **enteras** (o racionales) de $f(x_1,\ldots,x_n) = 0$ ó simplemente decidir si existe una tal solución, es uno de los problemas más antiguos de las matemáticas y tal vez uno de los más difíciles.

En el estudio de este tipo de problemas es necesario considerar también las soluciones **reales**, respectivamente complejas de la ecuación $f = 0$, es decir uno se ve confrontado con el estudio de la variedad algebraica compleja

$$V(f) = \left\{(x_1\ldots x_n) \in \mathbb{C}^n \mid f(x_1\ldots x_n) = 0\right\}$$

o también con la parte **real** de ella

$$V_{\mathbb{R}}(f) = \left\{(x_1\ldots x_n) \in \mathbb{R}^n \mid f(x_1\ldots x_n) = 0\right\}$$

Observación. Si $f(x_1,\ldots,x_n)$ es un polinomio **homogéneo** de grado m, es decir $i_1+\ldots+i_n = m \ \forall\ (i_1,\ldots,i_n)$, entonces obviamente $(0,\ldots,0)$ es una solución trivial la cual descartaremos. Además en este caso da lo mismo estudiar soluciones enteras o racionales, ya que $(a_1,\ldots,a_n)$ es solución si y sólo si $\forall\ \lambda \neq 0$, también $(\lambda a_1,\ldots,\lambda a_n)$ es solución de $f = 0$.

En el caso de polinomios homogéneos es más natural y conveniente estudiar las soluciones **proyectivas** de $f = 0$, es decir identificando $(a_1,\ldots,a_n)$ con $(\lambda a_1,\ldots,\lambda a_n)$, $\lambda \neq 0$ (siendo $(a_1,\ldots,a_n) \neq (0,\ldots,0)$) es decir se estudian las soluciones de $f = 0$ en el **espacio proyectivo** $\mathbb{P}^{n-1}$.

Sea $(a_1,\ldots,a_n) \in \mathbb{Z}^n$ una solución de $f = 0$, es decir

$$f(a_1,\ldots,a_n) = 0 \tag{2}$$

Si p es un primo cualquiera, es claro que (2) implica $\forall\ r \geq 1$

$$f(a_1,\ldots,a_n) \equiv 0 \pmod{p^r} \tag{3}$$

es decir las **congruencias** $f(x_1,\ldots,x_n) \equiv \pmod{p^r}$ tienen solución $\forall$ p primo $\forall\ r \geq 1$.

Notación Si a divide b escribiremos $b \equiv 0 \pmod{a}$. De modo que **resolver una congruencia** de la forma $f(x_1,\ldots,x_n) \equiv 0 \pmod{p^r}$ significa encontrar un tuplo $(b_1,\ldots,b_n) \in \mathbb{Z}$ tal que $p^r \mid f(b_1,\ldots,b_n)$. Esto también equivale a resolver la ecuación $f(x_1,\ldots,x_n) = 0$ en $\mathbb{Z}/p^r\mathbb{Z}$. Si $r = 1$, $\mathbb{Z}/p\mathbb{Z}$ es el cuerpo con p elementos y lo denotaremos por $\mathbb{F}_p$.

Se puede hacer la pregunta obvia:

Si para todo primo p y todo entero $r \geq 1$, la congruencia

$$f(x_1,\ldots,x_n) \equiv 0 \pmod{p^r} \tag{4}$$

es soluble, es entonces la ecuación

$$f(x_1,\ldots,x_n) = 0$$

soluble en $\mathbb{Z}$?

Si es así, diremos que f satisface el principio **local - global** (o también principio de Hasse-Minkowski). Se sabe que si f es homogéneo de grado ≤ 2, entonces f satisface el principio local - global. Para $gr(f) \geq 3$, en general f no tiene esta propiedad y es un problema fundamental encontrar obstrucciones para que f satisfaga o no el principio local global.

Ejemplo: La ecuación diofántica

$$3x^3 + 5y^3 + 7z^3 = 0$$

no tiene solución entera $\neq (0,0,0)$, pero si las congruencias

$3x^3 + 5y^3 + 7z^3 \equiv (\text{mod. } p^r)$ para todo p primo, $r \geq 1$.

Otro ejemplo sencillo de una ecuación que no admite solución entera (= global) es:
Sea p un primo. Entonces:

$$x^3 + py^3 + p^2z^3 = 0 \tag{5}$$

no tiene solución en $\mathbb{Z}$. Pues supongamos que la tuviera, y sea $(x,y,z) \in \mathbb{Z}^3 - \{(0,0,0)\}$ una tal solución, y sin restricción $(x,y,z) = 1$, pues la ecuación es homogénea. Pero $p|x$ necesariamente. Sea $px' = x$. Reemplazando:

$$p^3x'^3 + py^3 + p^2z^3 = 0$$

es decir $y^3 + pz^3 + p^2x'^3 = 0$

Esto implica $p|y$. Sea $y = py'$ se obtiene

$$p^3y'^3 + pz^3 + p^2x'^3 = 0$$

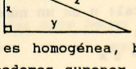
es decir $z^3 + px'^3 + p^2y'^3 = 0$

de modo que $p|z$. Esto contradice $(x,y,z) = 1$.

Como ya mencionamos el problema de resolver ecuaciones Diofánticas es uno de los más difíciles y atractivos de la teoría de números, particularmente porque involucra gran parte de la matemática. El propósito de estas charlas es mostrar con un ejemplo esta situación.

Comencemos con un ejemplo particularmente simple, cuya solución se obtiene vía divisibilidad elemental en los enteros: encontrar todos los **triángulos rectángulos con lados racionales**, es decir resolver en $\mathbb{Q}$ la ecuación

$$x^2 + y^2 = z^2 \tag{6}$$



Como esta ecuación es homogénea, basta resolverla en **enteros** (x,y,z). Además podemos suponer que x, y, z son relativamente primos $(x, y, z) = 1$ (se dice (x, y, z) es un triple pitagórico). De (6) se deduce que x e y tienen diferentes paridad y que z es necesariamente impar. Sea x par, y impar. Entonces:

$$x^2 = z^2 - y^2 = (z-y)(z+y)$$

con $z \pm y$ pares con $x = 2c$, $z + y = 2d$, $z - y = 2L$ se obtiene $c^2 = dl$, y por hipótesis $(d,l) = 1$. Del teorema fundamental de la aritmética se deduce de $c^2 = dl$ que d y l son ambos cuadrados, es decir $d = a^2$, $l = b^2$. Tenemos entonces $z + y = 2a^2$, $z - y = 2b^2$, $c^2 = a^2b^2$, es decir $c = ab$ (eligiendo un signo). De esto resulta:

$$x = 2ab$$
$$y = a^2 - b^2$$
$$z = a^2 + b^2$$

donde a,b son enteros arbitrarios. Hemos obtenido así **todos** las soluciones enteras (resp. racionales) de $x^2 + y^2 = z^2$. Este problema fue probablemente completamente resuelto por Diofantos.

Alrededor del siglo X, matemáticos árabes formularon el siguiente problema: Encontrar todos los triángulos rectángulos con lados racionales, cuya área sea **entera.**

DEFINICION

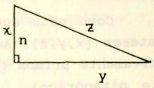
Todo entero n que es área de un triángulo rectángulo con lados racionales se llama un **número de congruencia.**

Por ejemplo: 6 es el área del triángulo (3,4,5).

Respuesta. 5 es el área del triángulo $(\frac{3}{2}, \frac{20}{3}, \frac{41}{6})$, es decir 5 y 6 son números de congruencia. Se puede demostrar que 1, 2, 3, 4 **no** son números de congruencia.

En general: n es un número de congruencia si y sólo si las ecuaciones

$$(*)_n \qquad \begin{aligned} x^2 + y^2 &= z^2 \\ \tfrac{1}{2}xy &= n \end{aligned}$$



tienen solución (x,y,z) en $\mathbb{Q}$.

En lo que sigue supondremos que n es un **entero libre de cuadrados.**

De $(*)_n$ se obtiene $\left(\frac{x \pm y}{2}\right)^2 = \left(\frac{z}{2}\right) \pm n$, de modo que con $t = \left(\frac{z}{2}\right)^2$, vemos que si n es de congruencia, existe $t \in Q$ tal que t, t+n, t-n son cuadrados. El inverso también es cierto.

Por ejemplo si 1 fuese número de congruencia, existiría un $t \in Q$ tal que t-1, t, t+1 son cuadrados. Se ve que esto implica que existen números enteros u, v, w con $u^4 - v^4 = w^2$, w impar. Demostrar (ejercicio) que esto no es posible.

Volvamos al caso general $(*)_n$. De las ecuaciones

$$\left(\frac{x \pm y}{2}\right)^2 = \left(\frac{z}{2}\right)^2 \pm n$$

$$\left(\frac{x^2 - y^2}{4}\right)^2 = \left(\frac{z}{2}\right)^4 \pm n^2$$

es decir, la ecuación $u^4 - n^2 = v^2$ tiene una solución racional con $U = \frac{z}{2}$, $v = \frac{x^2 - y^2}{4}$. Multiplicando por u^2 y reemplazando

$$X := u^2 = \left(\frac{z}{2}\right)^2$$

$$Y := uv = \frac{(x^2 - y^2)z}{8}$$

se obtiene que la ecuación (cúbica)

$$E_n: Y^2 = X^3 - n^2X$$

tiene una solución racional (X,Y), con la propiedad que $X = \left(\frac{z}{2}\right)^2$ es un cuadrado racional y que el denominador de X es par.

Se tiene en efecto que este hecho es una condición necesaria y suficiente para que n sea un número de congruencia, es decir

TEOREMA. Sea n un entero libre de cuadrados. Entonces n es un número de congruencia si y sólo si la ecuación cúbica

$$E_n: y^2 = x^3 - n^2x$$

tiene una solución racional (x,y) con $x \in Q^2$, cuadrado racional

y tal que el denominador de x es par.

Demostración. Basta demostrar que esta condición es suficiente. Sea $(x,y) \in \mathbb{Q}^2$ con $x \in \mathbb{Q}_+^2$, x con denominador par y tal que $y^2=x^3-n^2x$. Sea $u=\sqrt{x} \in \mathbb{Q}_+$, $v=\frac{y}{u}$, de modo que $v^2=x^2-n^2$. Así $v^2+n^2=x^2$. Sea t el denominador de u, es decir el entero > 0 más pequeño con $tu \in \mathbb{Z}$. Por hipótesis $t \in 2\mathbb{Z}$. Observemos que v^2, x^2 tienen el mismo denominador, pues n es entero con $v^2+n^2=x^2$. Este denominador es t^4.

Se tiene entonces $(t^2v)^2+(t^2n)^2=(t^2x)^2$, donde los enteros t^2v, t^2n, t^2x son relativamente primos. Además $t^2n \in 2\mathbb{Z}$ es par. Por la solución general de los triple pitagóricos se obtiene

$$t^2n = 2ab,\ t^2v = a^2 - b^2,\ t^2x = a^2 + b^2$$

con a, b enteros. Con $x = u^2$ se obtiene

$$t^2u^2 = a^2 + b^2, \text{ de modo que}$$

$$\left(\frac{2a}{t}\right)^2 + \left(\frac{2b}{t}\right)^2 = (2u)^2$$

define un triángulo rectángulo racional con área

$$\frac{1}{2} \cdot \frac{2a}{t} \cdot \frac{2b}{t} = \frac{2ab}{t^2} = n$$

es decir n es un número de congruencia.

Hemos reducido así el problema $(*)_n$ a estudiar la ecuación cúbica

$$E_n: y^2 = x^3 - n^2x$$

y encontrar todas las soluciones racionales $(x,y) \in \mathbb{Q}^2$ con $x \in \mathbb{Q}_+^2$, denominador de x par.

La ecuación E_n define lo que se entiende por una **curva elíptica** (racional). A continuación estudiaremos brevemente algunas propiedades geométricas y algebraicas de este tipo de curvas, lo cual nos permitirá traducir nuestro problema original $(*)_n$ en un problema básicamente analítico.

Consideremos la ecuación

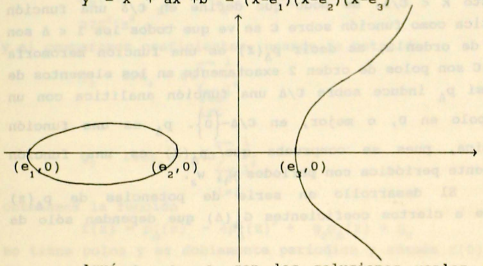
$$E: y^2 = x^3 + ax + b \qquad , a,b \in \mathbb{Q}$$

Se dice que E define una curva elíptica si el

discriminante del polinomio cúbico $\Delta=4a^3-27b^2$ es $\neq 0$ (A veces se usa $4x^3+ax+b$ lo cual reduce el discriminante a: a^3-27b^2). Se denota por $E(\mathbb{C})$ el conjunto $\left\{(x,y)\in\mathbb{C}x\mathbb{C} \mid y^2=x^3+ax+b\right\}$ de las soluciones complejas de E, al cual también se le agrega un punto $0 = \infty$, que corresponde a la solución $(0,1,0)\in\mathbb{P}^2(\mathbb{C})$ en el plano proyectivo, si se considera la ecuación homogénea $zy^2 = x^3 + axz^2 + bz^3$.

De este modo $E(\mathbb{C}) = \left\{(x,y)\in\mathbb{C}x\mathbb{C} \mid y^2=x^3+ax+b\right\}U\left\{0\right\}$, siendo la solución "escondida" de la ecuación en el infinito. Denotaremos por $e(Q) \subset E(\mathbb{C})$ el subconjunto de las soluciones **racionales**. En el plano $\mathbb{R}x\mathbb{R}$, el conjunto $E(\mathbb{R})$ es de la forma

$$y^2 = x^3 + ax + b = (x-e_1)(x-e_2)(x-e_3)$$

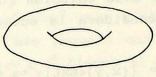


Aquí e_1, e_2, e_3 son las soluciones **reales** de la ecuación $x^3 + ax + b = 0$. Por supuesto que esta curva solo respresenta un **pedazo** de la curva elíptica compleja $y^2 = x^3 + ax + b$. El punto 0 no se puede vizualizar en el plano $\mathbb{R}^2$, y representa como "el punto en el infinito". El conjunto E(Q) son los puntos (x,y) del plano sobre la curva con coordenadas racionales, incluyendo el punto 0.

A continuación mencionaremos como es posible parametrizar los puntos de una curva elíptica via la función de Weirstrass.-

Sea $\Delta \subset \mathbb{C}$ un reticulado, es decir un subgrupo de

rango 2, $\Delta = \mathbb{Z}w_1 \oplus \mathbb{Z}w_2$ con $\{w_1, w_2\}$ linealmente independientes sobre $\mathbb{R}$. Entonces $\mathbb{C}/\Delta$ es un toro complejo, y como variedad real, de dimensión 2, es decir una superficie (compacta). Su imagen es simplemente



$\mathbb{C}/\Delta$ como variedad real

Asociada a Δ se tiene sobre $\mathbb{C}$ la siguiente función

$$(7) \qquad p_\Delta(z) = \frac{1}{z^2} + \sum_{\substack{l \in \Delta \\ l \neq 0}} \left[\frac{1}{(z-l)^2} - \frac{1}{l^2} \right]$$

la cual es absolutamente y uniformemente convergente en todo compacto $k \subset \mathbb{C}/\Delta$, de modo que define en $\mathbb{C}/\delta$ una función analítica como función sobre $\mathbb{C}$ se ve que todos los $l \in \Delta$ son polos de orden 2, es decir $p_\Delta(\mathbb{Z})$ es una función meromorfa sobre $\mathbb{C}$ son polos de orden 2 exactamente en los elementos de Δ. Así p_Δ induce sobre $\mathbb{C}/\Delta$ una función analítica con un solo polo en 0, o mejor, en $\mathbb{C}/\Delta - \{\bar{0}\}$. p_Δ es una función analítica, pues se comprueba que $p_\Delta(\mathbb{Z})$ es una función doblemente periódica con períodos w_1, w_2.

El desarrollo en serie de potencias de $p_\Delta(z)$ conduce a ciertos coeficientes $G_{2k}(\Delta)$ que dependen sólo de Δ.

$$(8) \qquad p_\Delta(z) = \frac{1}{z^2} + 3G_4(\Delta)z^2 + 5G_6(\Delta)z^4 + \quad 7G_8(\Delta)z^6 + \ldots$$

(sólo aparecen potencias pares de z, pues p_Δ es par).

Si $r > 2$ es un entero, se define

$$G_r = G_r(\Delta) = \sum_{\substack{l \in \Delta \\ l \neq 0}} \frac{1}{l^r}$$

y se comprueba que si $r \equiv 1(2)$, $G_r \equiv 0$. Estas son los coeficientes que aparecen en el desarrollo (8) de $p_\Delta(z)$. Esta series se llaman series de Eisenstein asociadas a Δ y

definen funciones que dependen de Δ.

De (8) se deduce

(9) $$p'_\Delta(z) = \frac{2}{z^3} + 6G_4 z + 20G_6 z^3 + 42G_8 z^5 + \ldots$$

de modo que

$$p'_\Delta(z)^2 = \frac{4}{z^6} - 24G_4 \frac{1}{z^2} - 80G_6 + (36G_4^2 - 16G_8)\, z^2 + \ldots$$

También tenemos

$$p_s(z)^2 = \frac{1}{z^4} + 6G_4 + 10G_6 z^2 + \ldots$$

$$p_s(z)^3 = \frac{1}{z^6} + 9G_4 \frac{1}{z^2} + 15G_6 + (21G_8 + 27G_4^2) z^2 + \ldots$$

y si comparamos coeficientes, usando la notación

$$g_2 = 60G_4 = 60 \sum_{\substack{l \in \Delta \\ l \neq 0}} \frac{1}{l^4}$$

$$g_3 = 140G_6 = 140 \sum_{\substack{l \in 0 \\ l \neq \Delta}} \frac{1}{l^6}$$

obtenemos la función

$$f(z) = p'_\Delta(z)^2 - 4p_\Delta(z)^3 + g_2 p_\Delta(z) + g_3$$

no tiene polos y es doblemente periódica y además $f(0) = 0$. De la teoría elemental de funciones se deduce $f(z) \equiv 0$, es decir

(10) $$p'_\Delta(z)^2 = 4p_\Delta(z)^3 - g_2 p_\Delta(z) - g_2$$

Obtenemos así que los puntos $(p_\Delta(z),\ p'_\Delta(z))$ están sobre la cúbica

$$E_\Delta: \quad y^2 = 4x^3 - g_2 x - g_3$$

El hecho que $\Delta = g_2^3 - 27g_3^2 \neq 0$, muestra que E_Δ es una curva elíptica. Se obtiene así una aplicación

$$\alpha: \mathbb{C}/\Delta \longrightarrow E_\Delta(\mathbb{C})$$

$$\overline{z} \longmapsto (p_\Delta(z),\ p'_\Delta(z)) \text{ si } \overline{z} \neq 0$$

$$0 \longmapsto 0 = \infty \qquad \text{si } \overline{z} = 0$$

la cual se demuestra, es **biyectiva**. Además si se consideran las estructuras de variedades analíticas de $\mathbb{C}/\Delta$ y $E_\Delta(\mathbb{C})$ se ve que α es un isomorfismo de variedades analíticas.

Inversamente, dados dos números $g_2, g_3 \in \mathbb{C}$ con $g_2^3 - 27g_3^2 \neq 0$, existe un reticulado $\Delta \subset \mathbb{C}$ tal que $g_2 = g_2(\Delta)$, $g_3 = g_3(\Delta)$, de modo que la curva elíptica $y^2 = 4x^3 - g_2x - g_3$ coincide con la curva E_Δ. Así el procedimiento anterior sirve para construir todas las curvas elípticas sobre $\mathbb{C}$.

Por otro lado $\mathbb{C}/\Delta$ tiene una estructura de **grupo abeliano**, de modo que mediante la biyección $\alpha: \mathbb{C}/\Delta \longrightarrow E_\Delta(\mathbb{C})$ podemos traspasar esta estructura de grupo a $E(\mathbb{C})$, es decir a los puntos de la curva elíptica $E: y^2 = 4x^3 - g_2x - g_3$. El elemento neutro de $E(\mathbb{C})$ será 0. Si $P = \alpha(\overline{z})$, $Q = \alpha(\overline{w})$, entonces

$$P + Q = \alpha(\overline{z+w})$$

Del hecho que $p(-z)=p(z)$, $p'(-z)=-p'(z)$ obtenemos por ejemplo: Sea $P=(x,y)=\alpha(\overline{z})$. Entonces $-P=\alpha(-\overline{z}) = (p(-z), p'(-z)) = (p(z), -p'(z))$ es decir $-P = (x, -y)$ es el punto simétrico de P sobre la curva E. Para encontrar las coordenadas de $P + Q$ en función de las de P y Q, se usa la siguiente fórmula clásica, llamada teorema de adición para la función $p(z)$:

(11) Para todo $z, w \in \mathbb{C}$, $z - w \notin \Delta$, $(z, w \notin \Delta)$

$$p(z + w) = -p(z) - p(w) + \frac{1}{4}\left[\frac{p'(z) - p'(w)}{p(z) - p(w)}\right]^2$$

Si $z-w \in \Delta$, es decir lo que equivale a calcular $p(2z)$ se tiene

(12)
$$p(2z) = -2p(z) + \frac{1}{4}\left[\frac{p''(z)}{p'(z)}\right]^2$$

(Usando (10) se calcula $p''(z)$ en función de $p'(z)$, $p(z)$).

Se tienen también fórmulas de adición para p', lo cual dejamos de ejercicio.

Poniendo $P_1=(x_1,y_1)$, $P_2=(x_2,y_2)$, $P_3=P_1+P_2 = (x_3,y_3)$, obtenemos para x_3 la siguiente fórmula correspondiente a (11),si $P_1 \neq P_2$ (respectivamente a (12) si $P_1 = P_2$):

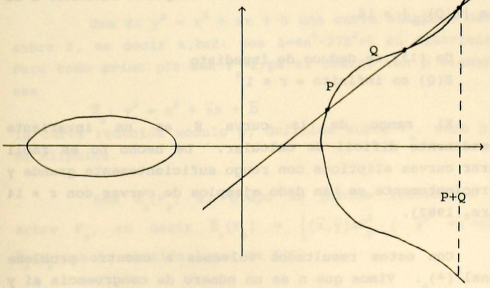
$$(11)' \quad x_3 = -x_1 - x_2 + \frac{1}{4}\left(\frac{y_1 - y_2}{x_1 - x_2}\right)^2 \qquad (P_1 \neq P_2)$$

$$(12)' \quad x_3 = -2x_1 + \frac{1}{4}\left(\frac{12x_1^2 - g_2}{2y_1}\right)^2 \qquad (P_1 = P_2)$$

Las coordenadas y_3 se obtienen de fórmulas similares para $p'(z+w)$ respectivamente $p'(2z)$.

La interpretación geométrica de estas fórmulas es evidente: Sean P_1, $P_2 \in E(\mathbb{C})$. Se une P_1 con P_2 por una recta la cual corta a E en un tercer punto P'. El punto simétrico de P' es $P_1 + P_2$. Si $P_1 = P_2$ se traza la tangente a E, la que corta a E en un punto P' y el punto simétrico de P es $2P_1$. El inverso -P de un punto P es simplemente el simétrico. El elemento neutro de $E(\mathbb{C})$ es el punto 0 en el infinito. Así tres puntos P_1, P_2, P_3 sobre $E(\mathbb{C})$ son colineales si y sólo si $P_1 + P_2 + P_3 = 0$.

Geométricamente obtenemos la siguiente figura



Una consecuencia de (11)', (12)' es la siguiente: Sea $Q \subseteq F \subseteq \mathbb{C}$ un cuerpo con g_2, $g_3 \in F$ (por ejemplo si g_2, g_3 son racionales, formamos Q). Sea $E(F) \subset E(\mathbb{C})$ el subconjunto de los puntos racionales sobre F, es decir con cooordenadas en F. De (11)', (12)' vemos que si P, $Q \in E(F)$, entonces también P + Q, 2P, tienen cooordenadas en F, es decir E(F) es un **subgrupo** de $E(\mathbb{C})$.

En particular

Si g_2, $g_3 \in Q$ entonces E(Q) es un grupo abeliano. Un teorema profundo de aritmética afirma

TEOREMA(Mordell)

E(Q) es finitamente generado, es decir existen puntos P_1, ..., $P_q \in E(Q)$ tal que todos los demás puntos de E(Q) (es decir las soluciones racionales de $y^2=4x^3-g_2x-g_3$) se obtienen a partir de P_1, ..., P_q por el proceso de formas secantes respectivamente tangentes y cortar la cúbica.

En consecuencia podemos escribir

(13) $$E(Q) = E(Q)_{tor} \oplus \mathbb{Z}P_1 \oplus \ldots \oplus \mathbb{Z}P_r$$

donde r = rango del grupo E(Q), $E(Q)_{tor}$ es el subgrupo de torsión de E(Q). Este subgrupo es finito, y recientemente B. Mazur demostró que para toda curva elíptica racional E se cumple $|E(Q)_{tor}| \leq 16$.

De (13) se deduce de inmediato

E(Q) es infinito $\Leftrightarrow r \geq 1$

El rango de la curva E es un invariante extremadamente difícil de calcular. De hecho no es fácil ncontrar curvas elípticas con rango suficientemente grande y solo recientemente se han dado ejemplos de curvas con $r \geq 14$ (Mestre, 1987).

Con estos resultados volvamos a nuestro problema original $(*)_n$. Vimos que n es un número de congruencia si y solo si la curva elíptica

E_n: $y^2 = x^3 - n^2x$

tiene un punto racional (x,y) con $x \in Q^2$, y denominador de x par. En $E_n(Q)$ se tiene fuera del elemento neutro los puntos obvios (0,0), (n,0), (-n,0) y se puede demostrar

$$(14) \qquad E_n(Q)_{tor} = \{0, (0,0), (n,0), (-n,0)\}$$

De este resultado y del anteriormente mencionado se deduce, ya que obviamente un punto racional $(x,y) \in E_n(Q)$ con $x \in Q^2$ y denominador de x par, no puede ser punto de torsión por (14), ya que si n es número de congruencia, entonces $E_n(Q) \neq E_n(Q)_{tor}$ y por lo tanto $r \geq 1$. En efecto se tiene:

Proposición

Sea r = rango de $E_n(Q)$. Entonces n es número de congruencia $\Leftrightarrow r \geq 1$.

De este modo hemos reducido nuestro problema a calcular el rango de $E_n(Q)$ (o mejor, a solo estimarlo por abajo).

Para estudiar este tipo de problemas introduciremos un nuevo objeto la **función Zeta** asociada a una curva elíptica. Esta función relaciona el comportamiento **local** de la curva elíptica con su comportamiento **global**.

Sea E: $y^2 = x^3 + ax + b$ una curva elíptica definida sobre $\mathbb{Z}$, es decir $a,b \in \mathbb{Z}$. Sea $\Delta = 4a^3 - 27b^2 \neq 0$ su discriminante. Para todo primo $p \nmid \Delta$ sea $F_p = \mathbb{Z}/p\mathbb{Z}$ el cuerpo con p elementos y sea

$$\overline{E}_p: y^2 = x^3 + \overline{a}x + \overline{b}$$

la curva reducida módulo p, definida sobre F_p. Como $p \nmid \Delta$, $\overline{E}_p$ es elíptica.

Sea $\overline{E}_p(F_p)$ el grupo de puntos racionales de $\overline{E}_p$ sobre F_p, es decir $\overline{E}_p(F_p) = \{(\overline{x},\overline{y}) \in F_p^2 \mid \overline{y}^2 = \overline{x}^3 + \overline{a}\overline{x} + \overline{b}\}$. $\overline{E}_p(F_p)$ es la versión **local** de E(Q).

Sea $N_1 = \#\bar{E}_p(F_p)$ el número de soluciones de $y^2 = \bar{x}^3 + \bar{a}x + \bar{b}$ en F_p, es decir usando congruencias tenemos:

$$N_1 = \# \left\{ (x,y) \in \mathbb{Z}x\mathbb{Z} \mid \begin{matrix} 0 \leq x,y \leq p-1 \\ p \mid y^2 - x^3 - ax - b \end{matrix} \right\} + 1$$

(+ 1 pues hay que contar el elemento neutro). El entero N_1 mide el número de soluciones locales en p de la ecuación $y^2 = x^2 + ax + b$.

Definamos $a_{E_p} = \dfrac{p + 1 - N_1}{2}$

para todo primo $p \nmid \Delta$

La función Zeta de E se define formalmente para $s \in \mathbb{C}$ por

$$(15) \qquad \xi_E(s) = \prod_{p \nmid \Delta} \frac{1}{1 - 2a_{E_p} p^{-s} + p^{1-2s}}$$

y se comprueba fácilmente que:

Proposición:

El producto (15) es uniformemente y absolutamente convergente sobre compactos en la región $Re(s) > \frac{3}{2}$, de modo $\xi_E(s)$ representa en este dominio una función analítica.

Si $Re(s) > \frac{3}{2}$, podemos desarrollar los factores locales $\dfrac{1}{1 - 2a_{E_p} p^{-s} + p^{1-2s}}$ en serie respecto a $\dfrac{1}{p^s}$ y multiplicarlos para todo $p \nmid \Delta$ y obtenemos un desarrollo en serie para $\xi_E(s)$.

$$(16) \qquad \xi_E(s) = \sum_{m=1}^{\infty} \frac{b_{E,m}}{m^s} \quad \text{con } b_{E,m} \in \mathbb{Z} \ \ \forall\, m \geq 1$$

es decir $\xi_E(s)$ es una **serie de Dirichlet** en el dominio $Re(s) > \frac{3}{2}$ con coeficientes enteros. Estos coeficientes $b_{E,m}$ también reflejan el comportamiento local de E, pero **toda la serie** refleja el comportameiento **global** de E. Por ejemplo

para E_1: $y^2 = x^3 - x$ se tiene:

(17) $$\xi_E(s) = 1 - \frac{2}{5^s} - \frac{3}{9^s} + \frac{6}{13^s} + \frac{2}{17^s} + \dots$$

y para E_n: $y^2 = x^3 - n^2x$, se tiene:

(18) $$\xi_{E_n}(s) = \sum_{m=1}^{\infty} \frac{b_{n,m}}{m^s}$$

donde

$$b_{n,s} = \left(\frac{n}{m}\right) b_{1,s}$$

con $b_{1,s}$ determinados por (17). Aquí $\left(\frac{-}{}\right)$ es el símbolo de Jacobi y vemos que conociendo $\xi_E(s)$ obtenemos $\xi_E(s)$ torciendo la serie por el carácter $\left(\frac{n}{}\right)$ de Jacobi.

Explícitamente (Re $s > \frac{3}{2}$)

(19) $$\xi_E(s) = 1 - 2\left(\frac{n}{5}\right)5^{-s} - 3\left(\frac{n}{3}\right)^2 9^{-s} + 6\left(\frac{n}{13}\right)13^{-s} + 2\left(\frac{n}{17}\right)17^{-s} + \dots$$

Una de las conjeturas más importantes en la aritmética de curvas elípticas es:

(BSD): $\xi_E(s)$ admite una prolongación analítica a todo el plano complejo y satisface una ecuación funcional. Además si r = rango de E(Q), entonces r satisface

$$\lim_{s \to 1} \frac{S_E(s)}{(s-1)^r} \neq 0$$

es decir r = **orden del cero** s = 1 de $\xi_E(s)$.

Esta conjetura fue originalmente formulada por Birch-Swinnerton Dyer.

En particular se puede dar la siguiente formulación **débil de esta conjetura:**

E(Q) es infinito $\Leftrightarrow$ $\xi_E(1) = 0$

Respecto a la prolongación analítica de $\xi_{E_n}(s)$ a todo $\mathbb{C}$ se puede demostrar que $\xi(s)$ tiene esta propiedad $\forall n \geq 1$ y que satisface una ecuación funcional. En consecuencia obtenemos:

Teorema

Suponiendo la conjetura débil de Birch-Swinnerton Dyer, se tiene para $n \geq 1$: n es número de congruencia $\Leftrightarrow$ $\xi_{E_n}(1) = 0$.

Ejemplo. El valor de $\xi_{E_n}(s)$ en s=1 sepuede calcular explícitamente via la teoría de formas modulares (de peso fraccionario) y se obtiene:

$$(20) \qquad \xi_{En}(1) = 2\sum_{m=1}^{\infty} \frac{b_{n,m}}{m} e^{\frac{-\pi m}{N}}$$

donde $N = \begin{cases} 2n\sqrt{2} & \text{sinesimpar} \\ 2n & \text{sinespar} \end{cases}$

En particular

$$\xi_{E1}(1) = 2\left(e^{-\pi/2\sqrt{2}} - \frac{2}{5} e^{-5\pi/2\sqrt{2}} - \frac{1}{3} e^{-9\pi/2\sqrt{2}} + \frac{6}{13} e^{-13\pi/2\sqrt{2}} + \frac{2}{17} e^{-17\pi/2\sqrt{2}} + R\right)$$

El resto R se puede estimar y el del orden

$$|R| \leq 0{,}012$$

de modo que se obtiene, al calcular las expresiones en el paréntesis

$$\xi_{E_1}(1) = 0{,}6555143... \pm 0{,}024$$

y es obvio que $\xi_{E_1}(1) \neq 0$. Esto confirma el hecho que 1 no es número de congruencia.

La expresión que hemos usado ((20)) para calcular $\xi_{E_n}(19)$ no proviene de la serie de Dirichlet $\sum \frac{b_{n,m}}{m^s}$, pues

esta serie sólo converge para $Re(s) > \frac{3}{2}$. La expresión que usamos proviene de la demostración de la prolongación analítica de $\xi_{E_n}(s)$ a $Re(s) > \frac{3}{2}$, la cual se obtiene de manera similar como se prolonga la función Zeta clásica de Riemann, es decir introduciendo una función teta adecuada de modo que $\xi_{E_n}(s)$ sea la transformada de Mellin de esta función teta.

Consideremos el anillo de enteros de Gauss $\mathbb{Z}[i] = \mathbb{Z} \oplus \mathbb{Z}i$, $i = \sqrt{-1}$. Para todo entero n se define un carácter

$$\chi_n : \mathbb{Z}[i] \longrightarrow \mathbb{C}$$

por

$$\chi_n(x) = \begin{cases} x\chi'(x)\left(\frac{n}{N(x)}\right) & \text{si } (x,2n)=1 \\ 0 & \text{si } (x,2n)\neq 1 \end{cases}$$

donde $N(a+bi) = a^2 + b^2$ es la norma de $x = a + bi$, y $\chi' : \mathbb{Z}[i] \longrightarrow \mathbb{C}$ se define por $\chi'(x) = i^r$, donde $i^r x \equiv 1 \bmod(2+2i)$ si $(x,2)=1$. Se comprueba que χ_n es una función multiplicativa y que si $Re(s) > \frac{3}{2}$

$$(21) \qquad \xi_{E_n}(s) = \frac{1}{4}\sum_{\substack{x \in \mathbb{Z}[i] \\ x \neq 0}} \frac{\chi_n(x)}{(N(x))^s}$$

Tal como para la función Zeta de Riemann, se puede preguntar si existe una función $F_{E_n}(t)$, $t \in \mathbb{R}_+$, tal que la transformada de Mellin de $F_{E_n}(t)$ sea $\pi^{-s}\Gamma(s)\xi_{E_n}(s)$, donde $\Gamma(s)$ es la función Γ usual, es decir, $\Gamma(s) = \int_0^\infty e^{-t} t^s \frac{dt}{t}$

Es decir, debe tenerse

$$(22) \qquad \pi^{-s}\Gamma(s)\xi_{E_n}(s) = \int_0^\infty t^s F_{E_n}(t) \frac{dt}{t}$$

En efecto, tal función existe y es la siguiente función teta:

$$(23) \qquad F_{E_n}(t) = \frac{1}{4}\sum \chi_n(x) e^{-\pi t|x|^2}$$

$$= \frac{1}{4}\sum_{m,n\in\mathbb{Z}} \chi_n(m+ni)e^{-\pi t(m^2+n^2)}$$

Tal como en el caso clásico de la función θ.

$$\theta(t) = \sum_{n=-\infty}^{\infty} e^{-\pi t n^2}$$

que satisface la ecuación funcional

$$\theta(t) = \frac{1}{\sqrt{t}}\theta\left(\frac{1}{t}\right)$$

la función $F_{E_n}(t)$ que hemos definido también satisface una ecuación funcional.

$$(24) \qquad F_{E_n}\left(\frac{1}{Nt}\right) = \begin{cases} \left(\frac{-2}{n}\right) Nt^2 F_{En}(t) & ,n \equiv 1(2) \\ \left(\frac{-1}{n_0}\right) Nt^2 F_{En}(t) & ,n = 2n_0 \end{cases}$$

donde N es el entero $\begin{cases} 8n^2 & \text{si} \quad n \equiv 1(2) \\ 4n^2 & \text{si} \quad n \equiv 0(2) \end{cases}$

Usando esta ecuación funcional y la expresión (22) se puede obtener la prolongación analítica de $\xi_{E_n}(s)$ a todo $\mathbb{C}$ y su ecuación funcional.

Supongamos $n \equiv 1, 2, 3 \ (8)$ para simplificar la ecuación funcional (24) de F_{E_n}; se obtiene:

$$(25) \qquad F_{E_n}\left(\frac{1}{Nt}\right) = Nt^2 F_{E_n}(t)$$

pues $\left(\frac{-2}{n}\right) = 1$ si $n \equiv 1, 2 \ (8)$, respectivamente $\left(\frac{-1}{n_0}\right) = 1$ si $n = 2n_0 \equiv 2 (\text{mod } 8)$. Usando (25) podemos escribir $\int_0^{\infty} F_{En}(t) t^s \frac{dt}{t}$ como suma de dos integrales desde $1/\sqrt{N}$ hasta ∞, permitiendo así eliminar la singularidad en $t = 0$.

Se tiene

$$\pi^{-s}\Gamma(s)\xi_{E_n}(s) = \int_0^\infty F_{E_n}(t)t^s\frac{dt}{t} = \int_{1/\sqrt{N}}^\infty F_{E_n}(t)t^s\frac{dt}{t} + \int_0^{1/\sqrt{N}} F_{E_n}(t)t^s\frac{dt}{t}.$$

Pero $1/\sqrt{N}$ es el centro de la ecuación funcional (25), de modo que si en la segunda integral hacemos la transformación $t \to \frac{1}{Nt}$ y usamos (25), para reemplazar $F_{E_n}\left(\frac{1}{Nt}\right)$ por $Nt^2F_{E_n}(t)$, obtenemos

$$(26) \qquad \pi^{-s}\Gamma(s)\xi_{E_n}(s) = \int_{1/\sqrt{N}}^\infty \left(t^sF_{E_n}(t) + N^{1-s}F_{E_n}(t)\right)\frac{dt}{t}$$

Se comprueba que usando (26) se puede extender $\xi_{E_n}(s)$ analíticamente a todo $\mathbb{C}$ y además se obtiene de inmediato la ecuación funcional siguiente:

$$(27) \qquad \left(\frac{\sqrt{N}}{\pi}\right)^s\Gamma(s)\xi_{E_n}(s) = \left(\frac{\sqrt{N}}{\pi}\right)^{2-s}\Gamma(2-s)\xi_{E_n}(2-s)$$

Estamos suponiendo $n = 1,2,3$ (8). Para $n = 5,6,7$, (mod8) se tiene la misma ecuación funcional, sólo que hay que poner un signo - en uno de los lados de la igualdad.

Haciendo $s=1$ en (26), obtenemos para $n = 1,2,3$ (4):

$$(28) \qquad \xi_{E_n}(1) = 2\pi\int_{1/\sqrt{N}}^\infty F_{E_n}(t)dt$$

Recordemos que:

$$\xi_{E_n}(s) = \frac{1}{4}\sum_{\substack{x\in\mathbb{Z}[i]\\ x\neq 0}}\frac{\chi_n(x)}{N(x)^s} \qquad (\text{Re } s > \tfrac{2}{3})$$

respectivamente

$$F_{E_n}(t) = \frac{1}{4}\sum_{x\in\mathbb{Z}[i]}\chi_n(x)e^{-\pi t|x|^2}$$

En particular la serie de Dirichlet que define $\xi_{E_n}(s)$, es decir $\xi_{E_n}(s) = \sum_{1}^{\infty} \frac{b_{n,m}}{m^s}$, se obtiene con esta notación por

$$b_{n,m} = \frac{1}{4} \sum_{\substack{x \in Z[i] \\ N(x)=m}} \chi_n(x)$$

y por lo tanto también

$$(29) \qquad F_{En}(t) = \sum_{m=1}^{\infty} b_{n,m} e^{-\pi t m}$$

Reemplazando (29) en (28) e integrando término a término obtenemos finalmente:

Proposición:

Si $n \equiv 1, 2, 3 \ (8)$, entonces

$$(30) \qquad \xi_{En}(1) = 2 \sum_{m=1}^{\infty} b_{n,m} e^{-\pi m / \sqrt{N}}$$

donde $\sqrt{N} = \begin{cases} 2n\sqrt{2} & , \text{ n impar} \\ 2n & , \text{ n par} \end{cases}$

Se puede además demostrar que:

$$|b_{n,m}| \leq \sigma_0(m) \sqrt{m}$$

donde $\sigma_0(m)$ = número de derivaciones de m.

Esta última cota permite a veces estimar el resto de la suma (30) cuando se ha calculado hasta cierto entero M, y así poder deducir por lo menos que en ciertos casos $\xi_{En}(1) \neq 0$.

Ejemplo. Para n = 1 se tiene:

$$\xi_{E_1}(1) = 2 \left| e^{-\pi/2\sqrt{2}} - \frac{2}{5} e^{-5\pi/2\sqrt{2}} - \right.$$

$$\frac{1}{3}e^{-9\pi/2\sqrt{2}} + \frac{6}{13}e^{-13\pi/2\sqrt{2}} + \frac{2}{17}e^{-17\pi/2\sqrt{2}}\Big) + R$$

y se calcula que $|R| \leq 0.023$. Se obtiene entonces:

$$\xi_{E_1}(1) = 0{,}6586 \ldots \pm 0{,}023 \ldots \neq 0$$

lo que coincide con el hecho que 1 no es número de congruencia.

Finalmente formularemos los resultados más recientes conocidos respecto a este problema, los que se deben a Tunnel (ver [T]). Usando la teoría de formas modulares de peso fraccionaria y la correspondencia de Shinima con las formas modulares de peso entero, Tunnel recientemente demostró la existencia de dos formas modulares de peso 3/2.

respectivamente $f(z)=\sum a_m q^m$, $\tilde{f}(z)=\sum \tilde{a}_m q^m$ $\quad (q = e^{2\pi i z})$

tal que a través de la correspondencia de Shinima

$$Sh(f) = Sh(\tilde{f}) = \sum b_{1,m} q^m$$

donde $\xi_{E_1}(s) = \sum_1^\infty \frac{b_{1,m}}{m^s}$. Además existe una constante β=2.622... tal que

(31) $$\xi_{E_n}(1) = \begin{cases} \frac{\beta}{4\sqrt{n}} a_n^2 & \text{si n es impar} \\ \frac{\beta}{2\sqrt{n}} \tilde{a}_{n/2}^2 & \text{si n es par} \end{cases}$$

En particular

(32) $$\xi_{E_n}(1) = 0 \Leftrightarrow \begin{cases} a_n^2 = 0 \text{ sinesimpar} \\ \tilde{a}_{n/2}^2 = 0 \text{sinespar} \end{cases}$$

En efecto las formas f, $\tilde{f}$ se pueden construir

explícitamente usando la función teta clásica

(32) $\quad \theta(z) = \sum_{n\in\mathbb{Z}} q^{n^2} \qquad (q = e^{2\pi i z})$

Concretamente se tiene:

$f(z) = (\theta(Z)-\theta(4z))(\theta(32z)-\frac{1}{2}\theta(8z))\theta(2z)$

$\tilde{f}(z) = (\theta(Z)-\theta(4z))(\theta(32z)-\frac{1}{2}\theta(8z))\theta(4z)$

Reemplazando (32) en estas expresiones se puede calcular explícitamente el valor de a_n, respectivamente $\tilde{a}_n$. se obtiene:

$$a_n = \#\left\{(x,y,z)\in\mathbb{Z}^3 \mid 2x^2 + y^2 + 32z^2 = n\right\}$$
$$- \frac{1}{2}\#\left\{(x,y,z)\in\mathbb{Z}^3 \mid 2x^2 + y^2 + 8z^2 = n\right\}$$

Resp. para n par

$$a_{\frac{n}{2}} = \#\left\{x,y,z)\in\mathbb{Z}^3 \mid 4x^2 + y^2 + 32z^2 = \frac{n}{2}\right\}$$

$$- \frac{1}{2}\#\left\{(x,y,z)\in\mathbb{Z}^3 \mid 4x^2 + y^2 + 8z^2 = \frac{n}{2}\right\}$$

Combinando este resultado con (31) y con la caracterización de los números de congruencia a través de los valores de $\xi_{E_n}(1)$, obtenemos finalmente:

Teorema

Sea n un entero > 0 libre de cuadrados. Suponiendo la conjetura débil de Birch-Swinnerton Dyer, se tiene la equivalencia de:

i) n es un número de congruencia

ii) Si n es impar

$$\#\left\{x,y,z)\in\mathbb{Z}^3 \mid 2x^2+y^2+32z^2=n\right\} = \frac{1}{2}\#\left\{(x,y,z)\in\mathbb{Z}^3 \mid 2x^2+y^2+8z^2=n\right\}$$

Si n es par

$$\#\left\{x,y,z)\in\mathbb{Z}^3 \mid 4x^2+y^2+32z^2=\frac{n}{2}\right\} = \frac{1}{2}\#\left\{(x,y,z)\in\mathbb{Z}^3 \mid 4x^2+y^2+8z^2=\frac{n}{2}\right\}$$

Observación:

Lo particularmente interesante de este resultado es que dado un entero cualquiera n, las condiciones del teorema se pueden comprobar **efectivamente**. La conjetura de Birch-Swinnerton Dyer para E_n se ha comprobado por Cross-Zagier para una clase grande de enteros, pero sigue siendo un problema abierto comprobarlo para todo n.

LITERATURA

I.- Introducción a la teoría de números:

W.J.Leveque. Fundamentals of Number Theory. Addison-Wesley, 1977.

N.Koblitz.Why study equations over finite fields?. Math. Magazine 55 (1982) 144-149.

G.H.Hardy and E.M.Wright. An introduction to the theory of numbers. Oxford Univ. Press (1960).

II.- Teoría de curvas elípticas:

J.W.S.Cassels.Diophantine equations with special reference to elliptic curves J.London Math.Soc. 41(1966) 193-291.

B.H.Gross. Arithmetic on elliptic curves with complex multiplication. LNM 776, Springer-Verlag, 1980.

S.Lang. Elliptic Functions. Addison - Wesley, 1973.

III.- El problema de números de congruencia

R. Alter. The Congruence number problem.
Am. Math. Monthly 87 (1980) 43-45.

N. Kablitz. Introduction to elliptic curves and modular forms. GTM 97, Springer (1984).

I. Tunnell. A classical diophantine problem and modular forms of weight 3/2.
Invent. Math. 72 (1983) 323-324.