GEOMETRIA DE LOS CASOS DE FACTOREO

Jorge Vargas

El objeto de este artículo es mostrar algunas aplicaciones geométricas de los casos de factoreo.

La letra F designará indistintamente el conjunto de los números racionales $\mathbb{Q}$, reales $\mathbb{R}$ o complejos $\mathbb{C}$ (Para el lector informado, F designará un cuerpo arbitrario de característica cero).

Un polinomio en una (dos, tres,...) variable a coeficientes en F es una expresión formal del tipo,

$$a_n X^n + a_{n-1} X^{n-1} + \ldots \qquad \text{(una variable)}$$

$$a_{nm} X^n Y^m + a_{n-1,m} X^{n-1} Y^m + \ldots \quad \text{(dos variables)}$$

Denotemos por $F[X]$ ($F[X,Y]$, $F[X,Y,Z]$,...) el conjunto de polinomios en una variable (dos variables, tres variables,...). Notar que $F[X] \subset F[X,Y] \subset F[X,Y,Z] \subset \ldots$. Por comodidad denotaremos por $F[\ldots]$ cualquiera de los conjuntos $F[X]$, $F[X,Y]$, $F[X,Y,Z]$,...

Observación: Como $\mathbb{R} \subset \mathbb{C}$ se tiene la inclusión $\mathbb{R}[\ldots] \subset \mathbb{C}[\ldots]$, esto es, todo polinomio a coeficientes reales puede pensarse como un polinomio a coeficientes complejos.

En la escuela media aprendimos a sumar y multiplicar polinomios y definimos:

Un polinomio no nulo P *divide* al polinomio Q si es posible encontrar un polinomio R tal que

$$Q = P.R$$

Ejemplo. $X^2 + Y$ *divide* a $X^4 - Y^2$ puesto que,

$$X^4 - Y^2 = (X^2 - Y)(X^2 + Y)$$

Claramente, un polinomio constante no nulo divide a cualquier polinomio P, por ejemplo: $\frac{\pi}{\sqrt{2}+\pi}$ divide a P puesto que,

$$P = \left(\frac{\sqrt{2}+\pi}{\pi} \cdot P \right) \frac{\pi}{\sqrt{2}+\pi}$$

También P divide a P puesto que $P = P.1$.

Un polinomio no constante P en $F[\ldots]$ se dice *primo* si los únicos divisores que tiene en $F[\ldots]$ son:

a) los polinomios constantes no nulos

b) los polinomios cP donde c es un elemento no nulo de F arbitrario.

Ejemplo: $X^2 + 1$ es primo en $\mathbb{R}[X]$ puesto que, si $X^2 + 1 = p(X)q(X)$ con $p(X) \in \mathbb{R}[X]$ y $q(X) \in \mathbb{R}[X]$, como el grado del producto es la suma de los grados de los factores resultan las alternativas,

grado (p) = grado (q) = 1

grado (p) = 2 y grado (q) = 0

Si se da la primera, entonces $p(X) = aX + b$ y $q(X) = cX + d$ con $a \neq 0$ y $c \neq 0$. Multiplicando y recordando que dos polinomios coinciden si y solo si sus coeficientes coinciden, resulta $a^2 + b^2 = 0$. Con la suma de dos números positivos nunca es nula, se tiene $a = b = 0$ lo cual es imposible. Esto concluye la justificación de que $X^2 + 1$

es primo en $\mathbf{R}[X]$. Sin embargo, $X^2 + 1$ no es primo en $\mathbf{C}[X]$ puesto que $X^2 + 1 = (X + i)(X - i)$ en $\mathbf{C}[X]$. Este ejemplo muestra que el hecho de que un polinomio sea primo depende del cuerpo donde pensemos a sus coeficientes.

Ejercicio. $P(X,Y,Z) = aX + bY + cZ$ es primo

$P(X,Y) = X^2 - Y$ o $P(X,Y) = X^2 + aY$ $(a \neq 0)$ son primos.

$P(X,Y) = Y + aX^2 + bY^2$ es primo.

$P(X,Y) = X^2 + Y^2$ es primo en $\mathbf{R}[X,Y]$ y no es primo en $\mathbf{C}[X,Y]$.

Para completar el panorama sobre polinomios primos en una variable probamos,

Proposición: a) Si $p \in F[X]$ tiene grado uno entonces, p es primo.

b) Si $p \in \mathbb{R}[X]$ tiene grado dos entonces, p es primo si y solo si su discriminante es negativo.

Prueba: a) Si $p(X) = aX + b$ con $a \neq 0$ y escribimos a p como producto de dos polinomios entonces, al menos uno de ellos tiene grado uno y el otro grado cero. Esto dice que p es primo.

b) Por ser p de grado dos, p es reducible si y solo si p se puede expresar como producto de dos polinomios de grado uno, esto es, si y solo si p tiene raíces reales, lo cual sabemos equivale a que su discriminante es no negativo.

Se puede probar que:

1) Si $p \in \mathbf{R}[X]$ es primo, entonces grado de p es uno o dos (ver [1] pag. 249).
2) Si $p \in \mathbb{C}[X]$ es primo, grado de p es uno (Teorema de Gauss, ver [1] pag. 248).

Ejercicio. 1) $X^3 + 2$ es primo en $Q[X]$.

2) De ejemplos de polinomios de grado dos o tres primos en $Q[X]$

3) Si $p(X)$ es primo en $Q[X]$ ¿será $P(X)$ primo en $\mathbb{R}[X]$?

Ahora enunciaremos un teorema que mostrará que los polinomios primos son los "atomos" del conjunto de todos los polinomios.

Teorema. Si p es un polinomio no primo en $F[\ldots]$ entonces existen polinomios primos $p_1, \ldots, p_r$ en $F[\ldots]$, tales que $p = p_1 \cdots p_r$.

Ejemplo. $X^2 - 1 = (X-1)(X+1)$ en $\mathbb{R}[X]$.

$X^3 - 1 = (X-1)(X^2+X+1)$ en $\mathbb{R}[X]$.

$X^3 + X^2 - X - 1 = (X+1)(X+1)(X-1)$ en $\mathbb{R}[X]$

$X^2 - Y^2 = (X-Y)(X+Y)$ en $\mathbb{R}[X]$

$X^4 + Y^2 = (X^2 - iY)(X^2 + iY)$ en $\mathbb{C}[X]$

Notar que en el ejemplo $X^3 + X^2 - X - 1 = (X+1)(X+1)(X-1)$ el factor primo $X+1$ ocurre dos veces. Por tanto, el teorema de descomposición puede reenunciarse así,

> Dado un polinomio p de grado mayor o igual a uno, es posible encontrar polinomios primos $p_1, \ldots, p_r$ distintos y números naturales $k_1, \ldots, k_r$ tales que
>
> $$p = p_1^{k_1} \cdots p_r^{k_r}$$

Otro hecho importante es el siguiente,

Teorema. (Unicidad de la descomposición en factores primos)
Si $p, p_1, \ldots, p_r, q_1, \ldots, q_s$ son polinomios a coeficientes en F, $p_1, \ldots, p_r$ son primos y distintos dos a dos, $q_1, \ldots, q_s$ son primos y distintos dos a dos y vale que,

$$p = p_1^{k_1} \cdots p_r^{k_r} = q_1^{t_1} \cdots q_s^{t_s}$$

Entonces, $r = s$, q_1 = algún p_i y t_1 = al correspondiente exponente k_i de p_i, q_2 = a otro p_i y t_2 = al correspondiente exponente k_i, etc.

Prueba. Ver [1] pag. 242.

Este teorema dice que, si de alguna forma descompusimos a p como producto de polinomios primos y también lo descompusimos usando un camino distinto, entonces los factores primos que obtuvimos son exactamente los mismos, como así también sus multiplicidades (ie. los exponentes a que aparecen elevados cada factor primo).

Una manera de descomponer un polinomio en producto de polinomios primos es usando los casos de factoreo. Por ejemplo,

$$\begin{aligned} aX^3 + 2bX^3 - aXY^2 - 2bXY^2 &= X(aX^2 + 2bX^2 - aY^2 - 2bY^2) \\ &= X\,[\,a(X^2 - Y^2) + 2b(X^2 - Y^2)\,] \\ &= X(X^2 - Y^2)\,(a + 2b) \\ &= (a + 2b)\,X(X - Y)\,(X + Y). \end{aligned}$$

Los teoremas anteriores nos dicen que si hubieramos usado cualquier otro camino para hacerlo, el resultado final sería el mismo.

Pregunta. Si f y g son polinomios en una variable ¿Cuándo es $H(X,Y) = f(X) - g(Y)$ primo en $F[X,Y]$?.

Por ejemplo, sugerimos probar:

1) $f(X) - f(Y) = (X-Y)q(X,Y)$
2) Si $f(X) = p(u(X))$ y $g(Y) = p(v(Y))$ entonces
$$f(X) - f(Y) = (u(X) - v(Y))\,M(X,Y)$$
3) Si grado (f) es coprimo con grado (g) entonces $f(X) - g(Y)$ es primo.
4) Si $f_1, \ldots, f_n$ son polinomios en una variable y $X_1, X_2, \ldots, X_n$ son variables distintas entonces,

$h(X_1, \ldots, X_n) = f_1(X_1) + f_2(X_2) + \ldots + f_n(X_n)$ es primo si $n \geq 3$. En particular $X^n + Y^k + Z^m$, con n, m y k no nulos, es primo.

Ahora describimos la parte geométrica de estos teoremas y por ende lo prometido sobre la geometría de los casos de factoreo.

Si P es un polinomio en *una* variable con coeficientes en F, un *cero* o una *raíz* de P en F es un elemento a de F tal que,

$$P(a) = 0$$

Ejemplos: a) 1 es un cero de $X^2 - 1$.

b) $X^2 + 1$ no tiene ceros en $\mathbb{R}$ puesto que, un número no negativo X^2 mas uno siempre es positivo.

c) $X^2 + 1$ tiene en $\mathbb{C}$ los ceros i y -i.

Ejercicios: a) Construir polinomios de grado 2,4,6,8, ... que no tengan ceros en $\mathbb{R}$.

b) a es un cero de P si y solo si (X-a) divide a P.

c) Usando el teorema de Gauss probar que todo polinomio en una variable a coeficientes complejos, tiene al menos un cero en $\mathbb{C}$.

d) Probar que todo polinomio a coeficientes reales de grado impar tiene al menos una raíz en R.

e) Si $P \in \mathbb{R}[X]$ y $a \in \mathbb{C}$ es una raíz de P, probar que $\bar{a}$ (el complejo conjugado de a) es una raíz de P.

f) Si $a \in \mathbb{C}$ probar que $(X-a)(X-\bar{a}) \in \mathbb{R}[X]$.

g) Usar el teorema de Gauss para probar que todo polinomio primo a coeficientes reales tiene grado uno o dos.

h) ¿A lo sumo cuantos ceros tiene un polinomio en una

variable?

i) Sea $P \in F[X]$ tal que grado $(P) \leq 3$. Probar que P es primo en $F[X]$ si y solo si P no tiene ceros en F.

Si $P \in F[X,Y]$, un cero de P es un par (a,b) de elementos de F tal que $P(a,b) = 0$.

Ejemplo. (1, -1) es un cero de $X^2 - Y^2$.

$(\sqrt{2}, \sqrt{3})$ es un cero de $X^2 - Y^2 + 1$

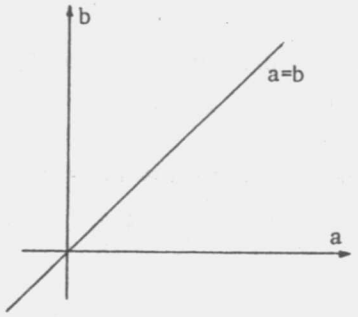
Si P es un polinomio en dos variables V(P) denotará el conjunto de ceros de P es decir,

$$V(P) = \{(a,b) \in FxF: P(a,b) = 0\}$$

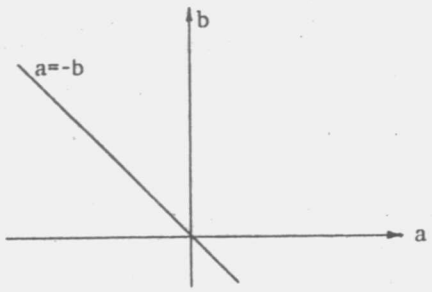
Ejemplos. a) Si $P(X,Y) = X-Y$,

$$V(P) = \{(a,b) \in FxF: a = b\}$$

Conjunto que dibujado en FxF ($\mathbf{R}^2$) resulta ser una recta.



b) Si $P(X,Y) = X+Y$, $V(P) = \{(a,b): a = -b\}$ es decir la recta indicada en el dibujo.



c) Si $P(X,Y) = X^2-Y^2$. Entonces $P(X,Y) = (X-Y)(X+Y)$. Ahora un producto de dos números es cero si y solo si uno de los factores lo es. Por lo tanto, $P(a,b) = (a-b)(a+b)$ es igual a cero si y solo si $a-b = 0$ o $a + b = 0$. Lo que permite concluir que $V(X^2-Y^2)$ es la unión de las rectas que obtuvimos en a) y b). Este ejemplo muestra un caso particular del siguiente resultado mas general.

Proposición. i) Si P es una potencia de un polinomio Q, entonces $V(P) = V(Q)$

ii) Si los factores primos distintos de P son $P_1, \ldots P_s$. Entonces $V(P) = V(P_1) \cup \ldots \cup V(P_s)$.

Prueba. i) Como $P(X,Y) = Q(X,Y)^m$ para algún entero positivo m, se tiene que $Q(a,b) = 0$ si y solo si $P(a,b) = Q(a,b)^m = 0$ lo cual dice que $V(P) = V(Q)$.

ii) Si $P_1, \ldots, P_s$ son los factores primos distintos de P, entonces vale que $P = P_1^{k_1} \ldots P_s^{k_s}$ con $k_1, \ldots, k_s$ enteros positivos fijos. Como $P(a,b) = P_1(a,b)^{k_1} \ldots P_s(a,b)^{k_s}$, y un producto de números es no nulo si y solo si al menos un factor lo

es, tenemos que $P(a,b) = 0$ si y solo si $P_j(a,b) = 0$ para algún j. Esto dice que $V(P) = V(P_1) \cup \ldots \cup V(P_s)$.

Esta proposición nos dice que para dibujar el conjunto de ceros de un polinomio, basta dibujar el conjunto de ceros de cada uno de sus factores primos. Como un posible método (cuando es aplicable) para encontrar los factores primos de un polinomio es usando los casos de factoreo, obtenemos así una aplicación a la geometría de los casos de factoreo.

Nota. Esta proposición vale no solamente para polinomios en dos variables, sino en una, dos, tres, cuatro, ... variables.

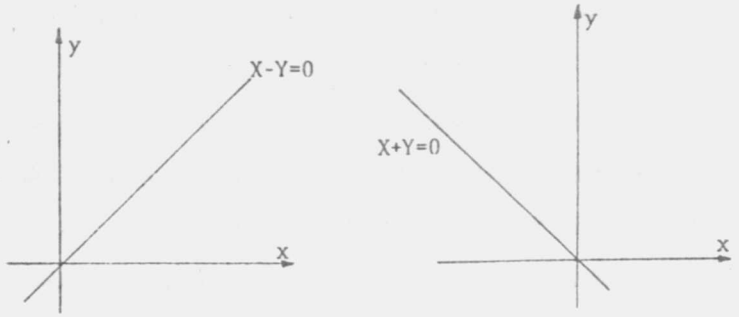
Ejemplo. Si $P(X,Y) = X^4 - Y^4$ sabemos que,

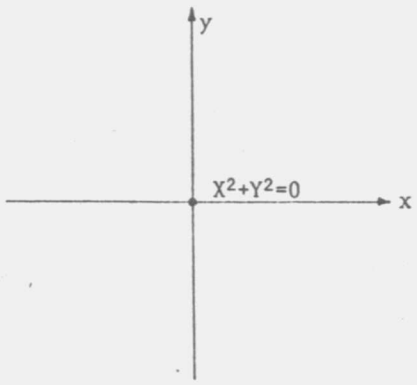
$$P(X,Y) = (X-Y)(X+Y)(X^2+Y^2)$$

y que esta es una factorización en primos en $\mathbf{R}[X,Y]$. Mientras que su factorización en primos en $\mathbf{C}[X,Y]$ es,

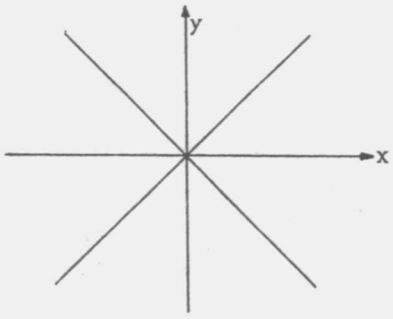
$$P(X,Y) = (X-Y)(X+Y)(X+iY)(X-iY).$$

Por la proposición anterior, o repitiendo la prueba de la proposición se tiene que el conjunto de ceros de P en $\mathbf{R} \times \mathbf{R}$ es la unión de, el conjunto de ceros de $X-Y$, con los ceros de $X+Y$, con los ceros de X^2+Y^2. Ahora en $\mathbf{R} \times \mathbf{R}$ se tiene que,





Por lo tanto el conjunto de ceros de X^4-Y^4 en **R** x **R** es,



Mientras que el conjunto de ceros de X^4-Y^4 en **C** x **C** es la unión de, los ceros de X-Y, con ceros de X+Y, con ceros de X+iY y ceros de X-iY. Esto es, el conjunto de ceros de X^4-Y^4 en **C** x **C** es la unión de las siguientes rectas en **C** x **C**, X = Y, X = -Y, X = iY, X = -iY.

Para mas ejemplos de polinomios reducibles o primos y el dibujo de sus ceros en **R** x**R**, sugerimos consultar [2] o, tomar cualquier libro de tercer año del secundario y de allí sacar ejemplos.

Ejercicios. 1) Cualquier recta en F x F es el conjunto de ceros de un polinomio de la forma P(X,Y) = AX+BY-C con $A \neq 0$ o $B \neq 0$.

2) P(X,Y) = AX + BY - C es un polinomio irreducible.

3) Si $P \in \mathbf{C}[\ldots]$ es un polinomio no constante entonces $V(P)$ es no vacío.

4) Si $P \in \mathbf{R}[\ldots]$ entonces $V(P)$ puede ser vacío.

Un teorema importante, debido a David Hilbert (1862-1943) dice lo siguiente, " *Si P es un polinomio irreducible en* $\mathbf{C}[\ldots]$ y Q *un polinomio que se anula en* $V(P)$ *(esto es, para todo* $(a,b) \in \mathbf{C} \times \mathbf{C}$ *tal que* $P(a,b) = 0$ *entonces,* $Q(a,b) = 0$*) entonces P divide a* Q".

(*Nota:* Aquí no hemos enunciado el resultado en su mayor generalidad). Por ejemplo, si Q es un polinomio que se anula en el conjunto de ceros de $P(X,Y) = X^2-Y$, entonces existe un polinomio R tal que $Q = (X^2-Y)R$. Notar que el resultado es falso en $\mathbf{R}[X,Y]$ puesto que, $X+Y$ se anula en $V(X^2+Y^2)$ y sin embargo X^2+Y^2 no divide a $X+Y$.

Una consecuencia de este teorema es el siguiente resultado.

Teorema. Si $P \in \mathbf{C}[X,Y]$ es un polinomio homogéneo entonces P se factorea como producto de polinomios primos del tipo $AX+BY$.

Bosquejo de la prueba: Recordemos que el grado de un monomio se define igual al natural que se obtiene al sumar los exponentes de cada variable y que un polinomio se dice homogéneo cuando todos sus monomios tienen el mismo grado.

Ejemplo. X^2+Y^2+XY es homogéneo.

X^2-Y+X no es homogéneo.

Ejercicio. Si $P(X,Y)$ es homogéneo y $P(a,b) = 0$ entonces $P(ta, tb) = 0$ para todo t en F.

Por lo tanto, si un polinomio homogéneo se anula en un punto de $\mathbf{C} \times \mathbf{C}$ se anula también en toda la recta que une dicho punto con el origen. Por un ejercicio anterior una tal recta es el conjunto de soluciones de un polinomio primo del tipo $AX+BY$. Por el teorema de Hilbert P tiene un factor del tipo $AX+BY$. Ahora, haciendo inducción sobre el

grado de P se prueba el teorema.

Ejercicios.

1) Factorear los siguientes polinomios en polinomios primos en $\mathbf{C}[X,Y]$.

$$X^3 - Y^3 + X^2Y, \quad X^3 + Y^3, \quad X^4 + Y^4, \quad X^2 + aXY + cY^2$$

$$X^5 + Y^5, \quad X^3 + 3XY^2 + 3X^2Y + Y^3, \quad X^n + Y^n$$

2) Factorear los polinomios $X^3 + Y^3 + Z^3$ y $X^2 + Y^2 + Z^2$ en $\mathbf{C}[X,Y,Z]$.

3) Comparar 1) y 2) ¿Qué conclusión se extrae?.

Miscelaneas.

En trigonometría aprendimos que los puntos de la circunferencia $x^2 + y^2 = 1$ (en nuestro lenguaje, los ceros del polinomio $P(X,Y) = X^2 + Y^2 - 1$) están parametrizados por el ángulo θ, y se tiene que

$$x = \cos\theta, \quad y = \operatorname{sen}\theta, \quad 0 \leq \theta \leq 2\pi$$

Es fácil verificar que todos los puntos de la circunferencia $x^2 + y^2 = 1$, salvo el $(1,0)$ están parametrizados por,

$$x = \frac{t^2 - 1}{t^2 + 1}, \quad y = \frac{-2t}{t^2 + 1}, \quad t \in \mathbf{R}$$

Surge entonces la siguiente pregunta. Dados P en $\mathbf{C}[X,Y]$ y su conjunto de ceros $V(P)$, ¿es posible encontrar funciones racionales de la variable t, $u(t)$ y $v(t)$ tales que,

$$(x,y) \in V(P) \text{ si y solo si } (x,y) = (u(t), v(t)) \text{ para algún } t \in \mathbf{C}$$

La respuesta parcial es,

1) Si grado de P es 2 entonces, si es posible.

2) Si grado de P es ≥ 3 puede que sí, puede que no. Por ejemplo,

$$y^2 = x^2 + x^3, \quad x = t^2 - 1, \quad y = t(t^2 - 1)$$

$$x^3 + y^3 = 1, \quad \text{no es posible.}$$

Bosquejo de la justificación de (1). Fijamos P primo y un punto $(x_o, y_o) \in V(P)$. Considerar la familia de rectas $y - y_o = t(x-x_o)$. Si $(x,y) \in V(P)$ entonces,

$$0 = P(x,y) = P(x,\ y_o + t\ (x-x_o))$$

Por lo tanto x y x_o son raíces de la ecuación de grado dos en X siguiente,

$$0 = P(X,\ y_o + t\ (X - x_o))$$

Dividimos esta ecuación por el coeficiente de X^2. Si A es el coeficiente de X en la ecuación resultante, entonces $A = x + x_o$ lo cual dice que $x = -A + x_o$. Ahora, reemplazando este valor de x en $y - y_o = t(x-x_o)$ obtenemos $y = y_o + t\ (-A)$. Como A es una función racional de t hemos probado (1).

Ejercicios. 1) Aplicar este proceso a: $x^2 + y^2 = 1$ con $(x_o,y_o) = (1,0)$ y a $y^2 = x^2 + x^3$ con $(x_o, y_o) = (0,0)$.

2) Probar que una parametrización de los ceros de $x^2 + y^2 = z^2$ está dada por,

$$x = 2uv, \quad y = u^2 - v^2, \quad z = u^2 + v^2 .$$

Notar que esta fórmula permite construir triángulos rectángulos.

3) Fije 2n números complejos $\alpha_1, \ldots, \alpha_{2n}$ con $\alpha_i \neq 0$ para cada i. Sea $a_i = \alpha_i + \frac{1}{\alpha_i}$. Mostrar que la función $(x,y) \to (u,v)$ con $u = x + \frac{1}{x}$, $v = \frac{y}{x^n}$ determina una función de V(P) en V(Q) donde,

$$P(X,Y) = Y^2 - \prod_{i=1}^{2n}(X - \alpha_i)(X - \frac{1}{\alpha_i})$$

$$Q(u,v) = v^2 - \prod_{i=1}^{2n}(u - a_i)$$

¿Es esta función racional?.

Un problema central en Matemática es el siguiente, "*Si* P(X,Y,...) *es un polinomio cuyos coeficientes son números enteros decribir los ce-*

ros enteros de P''.

Por ejemplo, es fácil ver que los ceros de $X^2 + Y^2 - Z^2$ son

$$x = r\,2uv, \quad y = r(u^2 - v^2), \quad z = r(u^2 + v^2)$$

los cuales son enteros si r, u y v lo son. La conjetura de Fermat (la cual todavía no ha sido probada) dice que, si $P(X,Y,Z) = X^n + Y^n - Z^n$ los únicos ceros enteros de P son:

1) Si n es par ≥ 3, $(\pm 1, 0, \pm 1)$ y $(0, \pm 1, \pm 1)$

2) Si n es impar ≥ 3, $(1,0,1)$ y $(0,1,1)$

Es un ejercicio relativamente fácil probar que $aX + bY - c$ tiene ceros enteros si y solo si el máximo común divisor de a y b divide a c. También es fácil describir los ceros de $aX + bY - c$ cuando existen. Se invita a los lectores a escribir artículos sobre estos temas.

Bibliografía

1) *Análisis Matemático I*. Vol I - Rey Pastor, Pi Calleja, Trejo - Editorial Kapelusz.

2) *Geometría Analítica*. - Santaló, Rey Pastor, Balanzat.

3) *Geometría Analítica*. Castelnuovo.

4) *Algebra Conmutativa*. Atiyah, Mc Donald.

Facultad de Matemática, Astronomía y Física
Universidad Nacional de Córdoba.