Cuatro Problemas de Algebra en la IMO.

Rafael Sánchez Lamoneda
UCV. Escuela de Matemáticas

Barquisimeto, 10 de Marzo de 2008

- **Introducción**. El objetivo de esta conferencia es analizar cuatro problemas de álgebra que han aparecido en las últimas IMO, con la idea de mostrarles unas técnicas útiles para la resolución de una amplia gama de problemas similares.

  A continuación les mostraré cuatro problemas que han aparecido en las últimas IMO. Las técnicas necesarias para resolverlos son básicas en un entrenamiento olímpico.

  Los conceptos necesarios para comprender las soluciones de los problemas son mínimos:

  - Noción de polinomio y grado
  - Ecuación de segundo grado
  - Divisibilidad

- **Problemas**

  - **Problema 1. (IMO 1988)**
    Sean a y b enteros positivos tales que $(ab+1)$ divide a a^2+b^2. Demostrar que
    $$\frac{a^2+b^2}{ab+1}$$
    es el cuadrado de un entero.
  - **Problema 2. (IMO 2007)**
    Sean a y b enteros positivos tales que $4ab-1$ divide a $(4a^2-1)^2$. Demostrar que $a=b$.
  - **Problema 3. (IMO 2006)** Sea $P(x)$ un polinomio de grado $n>1$ con coeficientes enteros y sea k un entero positivo. Considere el polinomio
    $$Q(x) = P(P(\ldots P(P(x))\ldots)),$$
    donde P aparece k veces.
    Demuestre que hay a lo sumo n enteros t, tales que $Q(t)=t$.

– **Problema 4. (IMO 2007)**
Sea n un entero positivo. Sea $I_n = \{0, 1, \ldots, n\}$. Se considera

$$S = \{(x, y, z) \ : \ x, y, z \in I_n, \ x + y + z > 0\}$$

como un conjunto de $(n+1)^3 - 1$ puntos en el espacio tridimensional.
Determinar el menor número posible de planos cuya unión contiene todos los puntos de S pero no incluye a $(0, 0, 0)$.

• **Soluciones a los Problemas**

– **Solución al Problema 1**
Procedemos por reducción al absurdo.
Si $ab + 1$ divide a $a^2 + b^2$, entonces existe un entero positivo k tal que:

$$\frac{a^2 + b^2}{ab + 1} = k.$$

Entonces: $a^2 - kab + b^2 = k$.
Supongamos que k no es un cuadrado perfecto.
En la expresión

$$a^2 - kab + b^2 = k,$$

ambos enteros, a y b son no nulos.
Si uno de ellos es cero, k es un cuadrado.
Además ambos tienen el mismo signo.
Si los signos son contrarios, entonces

$$ab < 0.$$

En consecuencia

$$a^2 - kab + b^2 > k.$$

Supongamos ahora que a y b son enteros tal que:

* $a^2 - kab + b^2 = k$,
* $a \geq b > 0$ y
* a mínimo con esa propiedad.

Esto no resta generalidad pues la ecuación es simétrica en a, b.
Observemos primero que $a > b$, pues si $a = b$, entonces
$(2 - k)a^2 = k$ y el lado izquierdo es no positivo.
Consideremos ahora la expresión

$$a^2 - kab + b^2 = k$$

como una ecuación cuadrática en a.
Ella tiene dos raíces a y a_1
y como $a + a_1 = kb$, entonces a_1 es un entero.

Tenemos entonces un nuevo par que satisface la ecuación, (a_1, b).
Por lo discutido antes,
como $b > 0$, entonces $a_1 > 0$.
Además $aa_1 = b^2 - k$, por lo tanto:

$$a_1 = \frac{b^2 - k}{a} < \frac{a^2 - 1}{a} < a.$$

En consecuencia:
El par (a_1, b) satisface la ecuación y

* $a_1 > 0$, $b > 0$, $a_1 < a$ y $b < a$,

lo cual contradice la minimalidad de a.
NOTA: Esta solución ganó premio a solución original en la IMO del año 1988.

- **Solución al Problema 2**

Procederemos de nuevo por reducción al absurdo.

Sean a y b números enteros positivos:
El par ordenado (a, b), es malo si y solo si

- $4ab - 1 | (4a^2 - 1)^2$ y
- $a \neq b$.

Como

$$b(4a^2 - 1)^2 - (4ab - 1)a(4a^2 - 1) = (a - b)(4a^2 - 1),$$

podemos afirmar que:

$$4ab - 1 | (4a^2 - 1)^2 \Rightarrow 4ab - 1 | (a - b)(4a^2 - 1).$$

Por otra parte, como $mcd(b, 4ab - 1) = 1$, entonces

$$\begin{aligned} 4ab - 1 | (a - b)(4a^2 - 1) &\Rightarrow 4ab - 1 | b(4a^2 - 1)^2 \\ &\Rightarrow 4ab - 1 | (4a^2 - 1)^2. \end{aligned}$$

Tenemos entonces que:

$$4ab - 1 | (4a^2 - 1)^2 \Leftrightarrow 4ab - 1 | (a - b)(4a^2 - 1).$$

Además:

$$4ab - 1 | (a - b)^2 \Leftrightarrow 4ab - 1 | (a - b)(4a^2 - 1).$$

En efecto:
Como $4ab-1$ divide a $(a-b)^2$, entonces:
$4ab-1|4a(a-b)^2+(4ab-1)(a-b)=(a-b)(4a^2-1)$,
por lo tanto, $4ab-1|(a-b)(4a^2-1)$.

Recíprocamente, como

$$4a(a-b)^2+(4ab-1)(a-b)=(a-b)(4a^2-1)$$

y

$$mcd(4a,4ab-1)=1,$$

entonces $4ab-1|(a-b)^2$.

En consecuencia por todo lo demostrado podemos concluir:

$$4ab-1|(4a^2-1)^2 \Leftrightarrow 4ab-1|(a-b)^2.$$

Tenemos entonces las siguientes equivalencias:

$$\begin{array}{rcl}(a,b)\ malo & \Leftrightarrow & 4ab-1|(a-b)^2\\ & \Leftrightarrow & 4ba-1|(b-a)^2\\ & \Leftrightarrow & (b,a)\ malo.\end{array}$$

Supongamos ahora sin pérdida de generalidad que tenemos un par malo (a,b) tal que $a>b$ y a es mínimo con esta propiedad.
(¿Por qué no se pierde generalidad?)

Como $4ab-1|(a-b)^2$, existe $m\in\mathbb{Z}^+$, tal que $(a-b)^2=m(4ab-1)$. Desarrollando y despejando convenientemente nos queda:

$$a^2-(4bm+2b)a+(b^2+m)=0.$$

Si analizamos esta expresión como una ecuación cuadrática en a, ella tiene una raiz entera (el entero a del par (a,b)) y por lo tanto su discriminante es un cuadrado perfecto. Es decir la expresión $(4bm+2b)^2-4(b^2+m)$ o bien $4(4mb^2+4b^2m^2-m)$, es un cuadrado perfecto.

Pero entonces existe un entero positivo t tal que:

$$4mb^2+4b^2m^2-m=(2mb+t)^2=4m^2b^2+4mbt+t^2.$$

Es decir:

$$m(4b^2-4bt-1)=t^2.$$

Como $m\in\mathbb{Z}^+$, entonces $0<t<b$ y podemos decir que existe $s\in\mathbb{Z}^+$ con $b>s>0$ y $s+t=b$, o bien $t=b-s$.

Sustituyendo tenemos:

$$m(4b^2 - 4b(b-s) - 1) = (b-s)^2$$
$$m(4bs - 1) = (b-s)^2.$$

Por lo tanto el par (b, s) es malo con $b < a$ y esto es una contradicción.

- **Solución al Problema 3**

  Como primera observación es claro que si toda raiz entera de $Q(x) - x$ es raiz de $P(x) - x$, como el grado de $P(x)$ es n, no hay nada que demostrar.

  Supongamos que este no es el caso, es decir existe $x_0 \in \mathbb{Z}$ tal que $Q(x_0) = x_0$ pero $P(x_0) \neq x_0$.

  Ahora definamos inductivamente la sucesión

  $$x_{i+1} = P(x_i),$$

  para $i = 0, 1, 2, \ldots$.

  Recordemos que por ser $P(x)$ un polinomio con coficientes enteros, entonces para todo par de números enteros diferentes u y v se cumple que $u - v$ divide a $P(u) - P(v)$.

  En consecuencia en la sucesión de diferencias no nulas:

  $$x_0 - x_1,\ x_1 - x_2,\ \ldots,\ x_{k-1} - x_k,\ x_k - x_{k+1}.$$

  cada término es un divisor del siguiente.

  Además $x_0 - x_1 = x_k - x_{k+1}$.

  Por lo tanto todas las diferencias tienen el mismo valor absoluto.

  Si denotamos $x_m = min(x_1, \ldots, x_k)$, entonces lo anterior implica:

  $$x_{m-1} - x_m = -(x_m - x_{m+1}).$$

  Por lo tanto: $x_{m-1} = x_{m+1}$.

  Pero entonces las diferencias consecutivas en la sucesión tienen signos opuestos y por la definición de los términos de la sucesión, es decir, $x_{i+1} = P(x_i)$, y $x_k = x_0$, podemos ahora concluir que la sucesión inicial $x_0, x_1, \ldots, x_k$, es una sucesión conformada por dos valores distintos que se alternan, es decir, una sucesión de la forma:

  $$x_0, x_1, x_0, x_1, \ldots, x_0, x_1, x_0.$$

  En otras palabras: Cada entero que queda fijo por $Q(x)$, también queda fijo por $P(P(x))$.

Para finalizar deberemos entonces demostrar que hay cuando más **n** números enteros que satisfacen esta condición.

Sea a un entero tal que $Q(a) = a$, pero $P(a) = b \neq a$. Entonces $P(b) = P(P(a)) = a$.

Sea α cualquier otro número entero que queda fijo por $P(P(x))$ y sea $P(\alpha) = \beta$. Además por lo que hemos discutido, $P(\beta) = \alpha$.

Observación: Los números α y β no tiene por qué ser distintos, pero lo que si ocurre es que son diferentes de a y b.

Como $\alpha - a | P(\alpha) - P(a) = \beta - b$ y $\beta - b | P(\beta) - P(b) = \alpha - a$, entonces:

$$\alpha - a = \pm(\beta - b).$$

Analogamente:

$$\alpha - b = \pm(\beta - a).$$

Supongamos que en ambas igualdades ocurre a la vez el signo $+$. Entonces: $\alpha - b = \beta - a$ y $\alpha - a = \beta - b$. Al restar obtenemos una contradicción, $a - b = b - a$, pues $a \neq b$.

Por lo tanto en las igualdades de antes, al menos una vale con signo $-$.

Cualquiera sea el caso esto significa que:

$$\alpha + \beta = a + b.$$

Equivalentemente:

$$P(\alpha) + \alpha - a - b = 0$$

Denotemos $c = a + b$, entonces hemos demostrado que cualquier entero que quede fijo por $Q(x)$ distinto de a y b es una raiz del polinomio $R(x) = P(x) + x - c$. Esto también es cierto para a y b, como se puede combrobar con el cálculo directo.

Como $P(x)$ es un polinomio de grado $n > 1$, también $R(x)$ tiene grado $n > 1$ y por lo tanto no puede tener más de **n** raíces.

- **Solución al Problema 4**

  Sea $i = 1, 2, \ldots, n$. Consideremos los $3n$ planos de ecuación

  $$x = i,\ y = i,\ z = i.$$

  Es claro que $(0, 0, 0)$ no pertenece a ninguno de ellos y además S está contenido en la unión de estos $3n$ planos.

  (También S está contenido en la unión de todos los planos de ecuación $x + y + z = k$ para $k = 1, 2, \ldots, n$).

Demostremos que $3n$ es la menos cantidad posible de planos.

Para poder demostrar que $3n$ es el número mínimo de planos que contienen a S, utilizaremos el si -guiente

- **Lema**

  Consideremos un polinomio no nulo $P(x_1, \ldots, x_k)$ en k variables. Supongamos que P se anula en todos los puntos $(x_1, \ldots, x_k)$ que satisfacen las tres condiciones siguientes:

  - $x_1, \ldots, x_k \in \{0, 1 \ldots, n\}$
  - $x_1 + \cdots + x_k > 0$
  - $P(0, \ldots, 0) \neq 0$.

  Entonces $grad(P) \geq kn$.

  Antes de dar una demostración del lema, veamos como se aplica:

  Supongamos que existen N planos cuya unión contiene al conjunto S pero ninguno de ellos pasa por el origen.

  Las ecuaciones de estos planos son de la forma:

$$a_i x + b_i y + c_i z + d_i = 0$$

  con $i = 1, 2, \ldots, N$ y todo $d_i \neq 0$.

  Consideremos el polinomio de grado N

$$P(x, y, z) = \prod_{i=1}^{N} (a_i x + b_i y + c_i z + d_i).$$

Claramente para todo $(x_0, y_0, z_0) \in S$,

$$P(x_0, y_0, z_0) = 0 \ y \ P(0, 0, 0) \neq 0$$

Por el lema concluimos que:

$$N = grad(P) \geq 3n,$$

y el problema está resuelto.

Nos queda entonces demostrar el lema.

- **Demostración del Lema**

  La demostración es por inducción sobre k.

  Como $P \neq 0$, el caso $k = 1$ es claro, pues si P se anula en todos los puntos $x_i \in \{1, \ldots, n\}$, entonces el grado de P es al menos n.

  Consideremos el polinomio

  $$Q(y) = y(y-1)\ldots(y-n).$$

  Entonces al dividir $P(x_1, \ldots, x_{k-1}, y)$ entre $Q(y)$ tenemos:

  $$P(x_1, \ldots, x_{k-1}, y) = Q(y)H + R(x_1, \ldots, x_{k-1}, y).$$

  Como $Q(y)$ se anula en cada $y = 1, 2, \ldots, n$,
  entonces:

  $$P(x_1, \ldots, x_{k-1}, y) = R(x_1, \ldots, x_{k-1}, y),$$

  para todo $x_1, \ldots, x_{k-1}, y \in \{0, 1, \ldots, n\}$.

  Por lo tanto R también satisface las hipótesis del lema y además $grad_y R \leq n$, pues $grad(Q(y)) = n + 1$.

  Como $gradR \leq gradP$, entonces es suficiente demostrar que $gradR \geq nk$.

  Escribamos R como un polinomio en y.

  $$\begin{array}{rcl} R(x_1, \ldots, x_{k-1}, y) & = & R_n(x_1, \ldots, x_{k-1})y^n + \ldots \\ & \ldots & +R_0(x_1, \ldots, x_{k-1}). \end{array}$$

  Si $R_n(x_1, \ldots, x_{k-1})$ satisface la hipótesis de inducción, entonces:

  $$gradR_n(x_1, \ldots, x_{k-1}) \geq (k-1)n,$$

  y en consecuencia

  $$gradP \geq gradR \geq gradR_n + n \geq kn.$$

  Nos queda entonces demostrar que $R_n(x_1, \ldots, x_{k-1})$ satisface la hipótesis de inducción. A saber:

– $R_n(0,\ldots,0) \neq 0$ y
– $R_n(x_1,\ldots,x_{k-1}) = 0$,

para todo $x_1,\ldots,x_{k-1} \in \{0,1,\ldots,n\}$ tal que $x_1+\cdots+x_{k-1} > 0$.

Sea $T(y) = R(0,\ldots,0,y)$. El grado de $T(y)$ es menor o igual a n, pues $grad_y R \leq n$.

Más aún:
$T(0) = R(0,\ldots,0,0) \neq 0$ y además $T(y) = 0$ para $y \in \{1,\ldots,n\}$. Por lo tanto su grado es n.

Pero entonces por la definición de $T(y)$ tenemos que:

$$R_n(0,\ldots,0,0) \neq 0.$$

Tomemos $k-1$ enteros $a_1,\ldots,a_{k-1} \in \{0,1,\ldots,n\}$ tales que $a_1+\cdots+a_{k-1} > 0$.

Sustituyendo $x_i = a_i$ en $R(x_1,\ldots,x_{k-1},y)$,
obtenemos un polinomio en y de grado a lo sumo n y que se anula en todos los puntos $y = 0,1,,\ldots,n$.

Por lo tanto este polinomio es nulo y sus coeficientes son iguales a cero, ie.,

$$R_i(a_1,\ldots,a_{k-1}) = 0$$

para todo $i = 0,1,\ldots,n$.
En particular:

$$R_n(a_1,\ldots,a_{k-1}) = 0,$$

con $a_1+\cdots+a_{k-1} > 0$.

En el caso especial $m = n$, hay una forma más fuerte de este teorema conocida como el Combinatorial Nullstellensatz.

- **Teorema (N. Alon)**

  Sea F un cuerpo arbitrario, y sea $f = f(x_1,\ldots,x_n)$ un polinomio en $F[x_1,\ldots,x_n]$. Sean $S_1,\ldots,S_n$ subconjuntos finitos no vacíos de F y defina $g_i(x_i) = \prod_{s\in S_i}(x_i - s)$. Si $f(s_1,\ldots,s_n) = 0$, para todo $s_i \in S_i$, entonces existen polinomios $h_1,\ldots,h_m$ en $F[x_1,\ldots,x_n]$, que satisfacen $grad(h_i) \leq grad(f) - gradg_i$ tal que:

$$f = \sum_{i=1}^{n} h_i g_i.$$

  Más aún, si para algún subanillo R de F, $f, g_1,\ldots,g_n \in R[x_1\ldots,x_n]$, entonces existen polinomios $h_i \in R[x_1\ldots,x_n]$, como antes.

  Como una consecuencia de este teorema tenemos

- **Teorema (N. Alon)**

  Sea F un cuerpo arbitrario, y sea $f = f(x_1, \ldots, x_n)$ un polinomio en $F[x_1, \ldots, x_n]$. Supongamos que $grad(f) = \sum_{i=1}^{n} t_i$, donde cada t_i es un entero no negativo y además el coeficiente de $\prod_{i=1}^{n} x_i^{t_i}$ en f es no nulo. Entonces si $S_1, \ldots, S_n$ subconjuntos de F con $|S_i| > t_i$, existen $s_1 \in S_1$, $s_2 \in S_2$, $\ldots$, $s_n \in S_n$, para los cuales:

  $$f(s_1, \ldots, s_n) \neq 0.$$

- **Corolario**

  PROBLEMA 4

- **Demostración**

  ¡Ejercicio!

- **Bibliografía.**

  Se puede consultar sobre el Combinatorial Nullstellensatz en:

  Combinatorics, Probability and Computing. Vol 8. Issue 1-2. January 1999. pg 7-29. Cambridge Univ. Press. NY. USA. ISSN 0963-5483.