

Lista de Ejercicios 2

ejercicio 1

Por Pablo Rojas

Demostrar el lema de Schwartz-Zippel

- Se tiene el polinomio $p(x_1, \dots, x_n)$ de grado k .
- El conjunto finito no vacío A tal que $A \in \mathbb{Q}$.
- $a_1, \dots, a_n$ elejidos de manera uniforme en A .

$$\Pr(p(a_1, \dots, a_n) = 0) \leq \frac{k}{|A|}$$

Resumen

- $p(x_1, \dots, x_n)$ polinomio
- k grado
- A subconjunto
- $a_1, \dots, a_n$ elegidos uniforme

$$\Pr(p(a_1, \dots, a_n) = 0) \leq \frac{k}{|A|}$$

Metodologia de resolución

- Demostrar cuando el polinomio es de una sola variable
- Luego usar eso para demostrar cuando para polinomios de múltiples variables

Cave notar

- Solo es util cuando :

$$k \leq |A|$$

- Eso es porque solo así se cumple:

$$\frac{k}{|A|} \leq 1$$

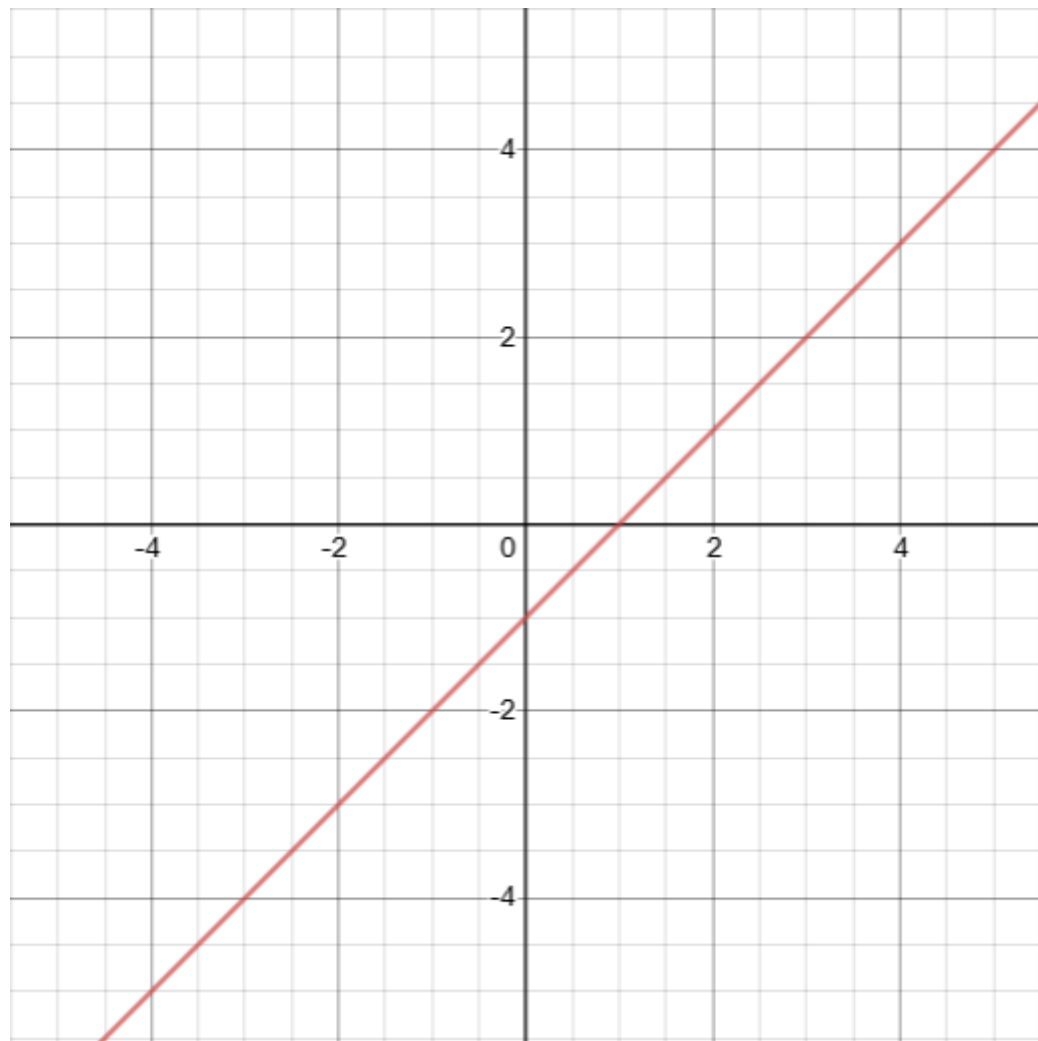
No hay probarilidades mayores a 1

Soluciones para un polinomio de 1 variable

- Es igual al grado k

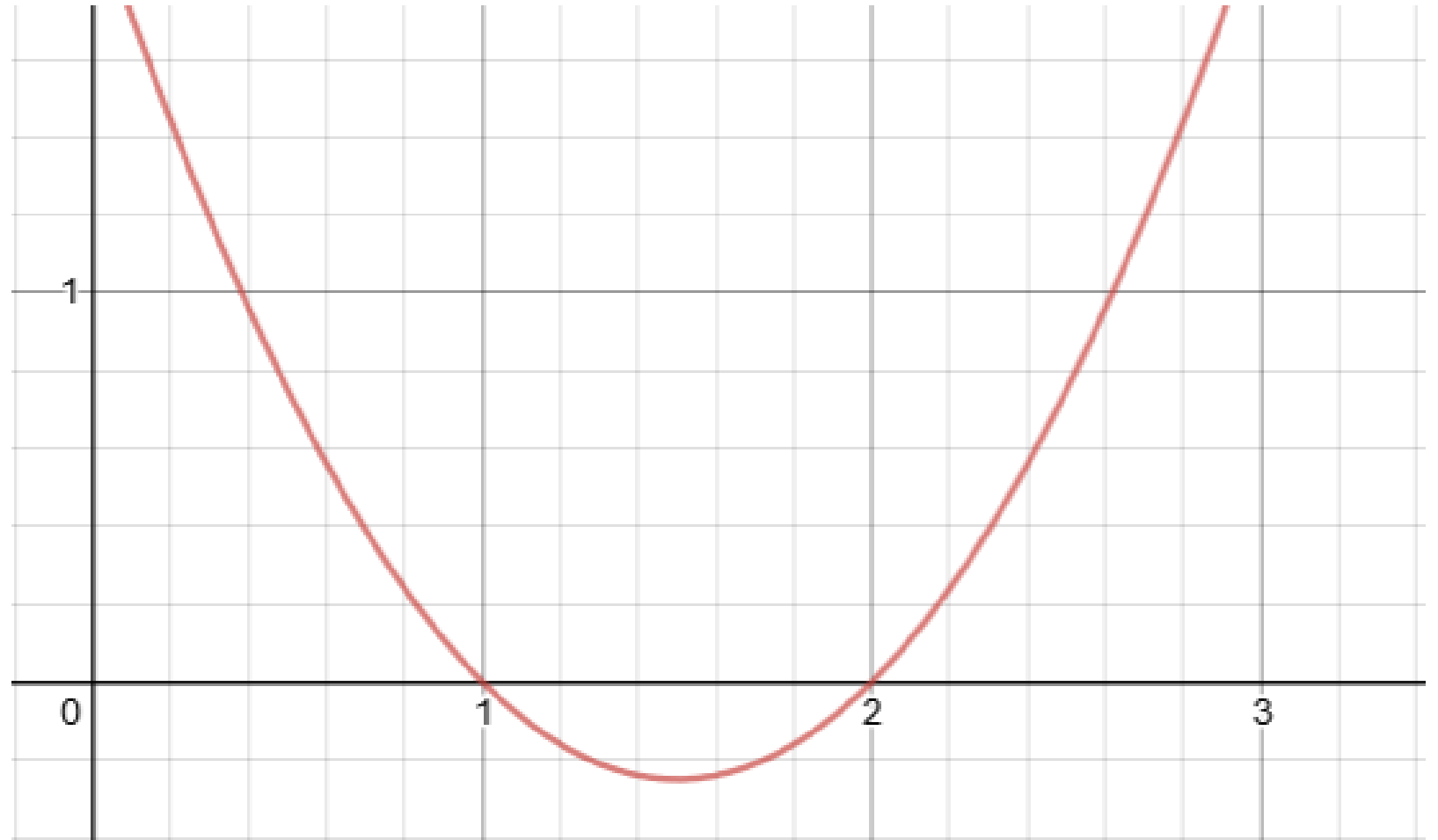
Ejemplos

- $x - 1$:



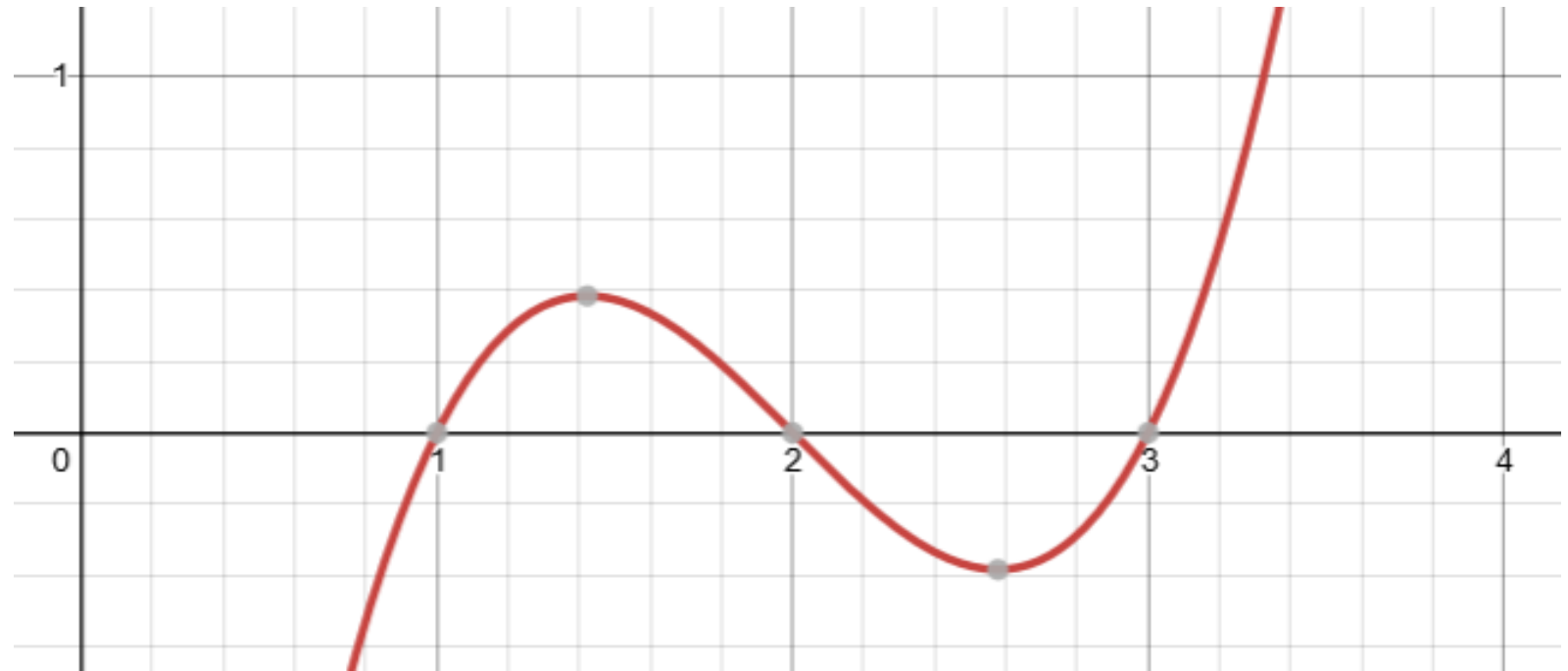
Ejemplos

- $x^2 - 3x + 2 =$
- $(x - 1)(x - 2)$



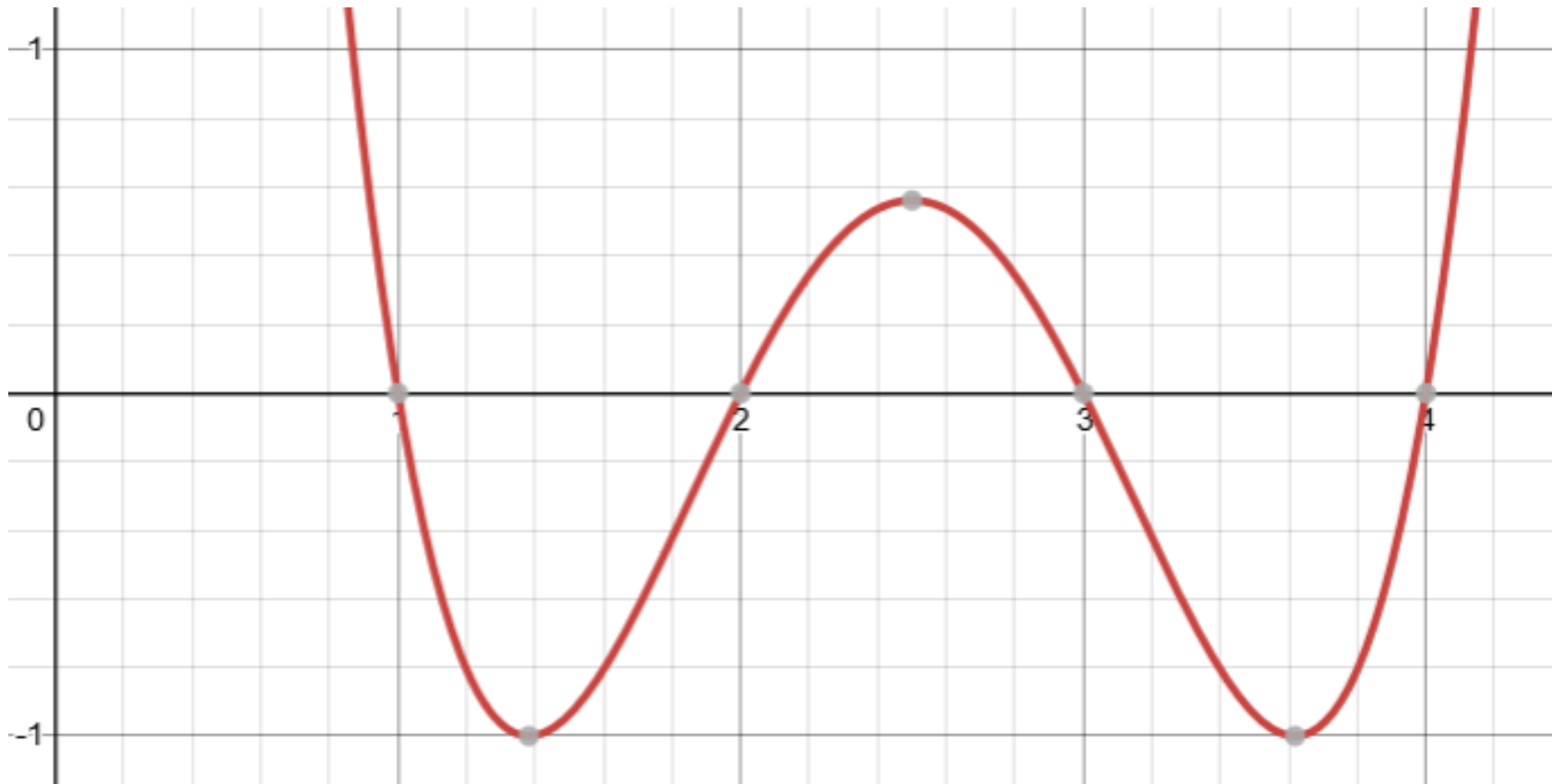
Ejemplos

- $x^3 - 6x^2 + 11x - 6 =$
- $(x - 1)(x - 2)(x - 3)$

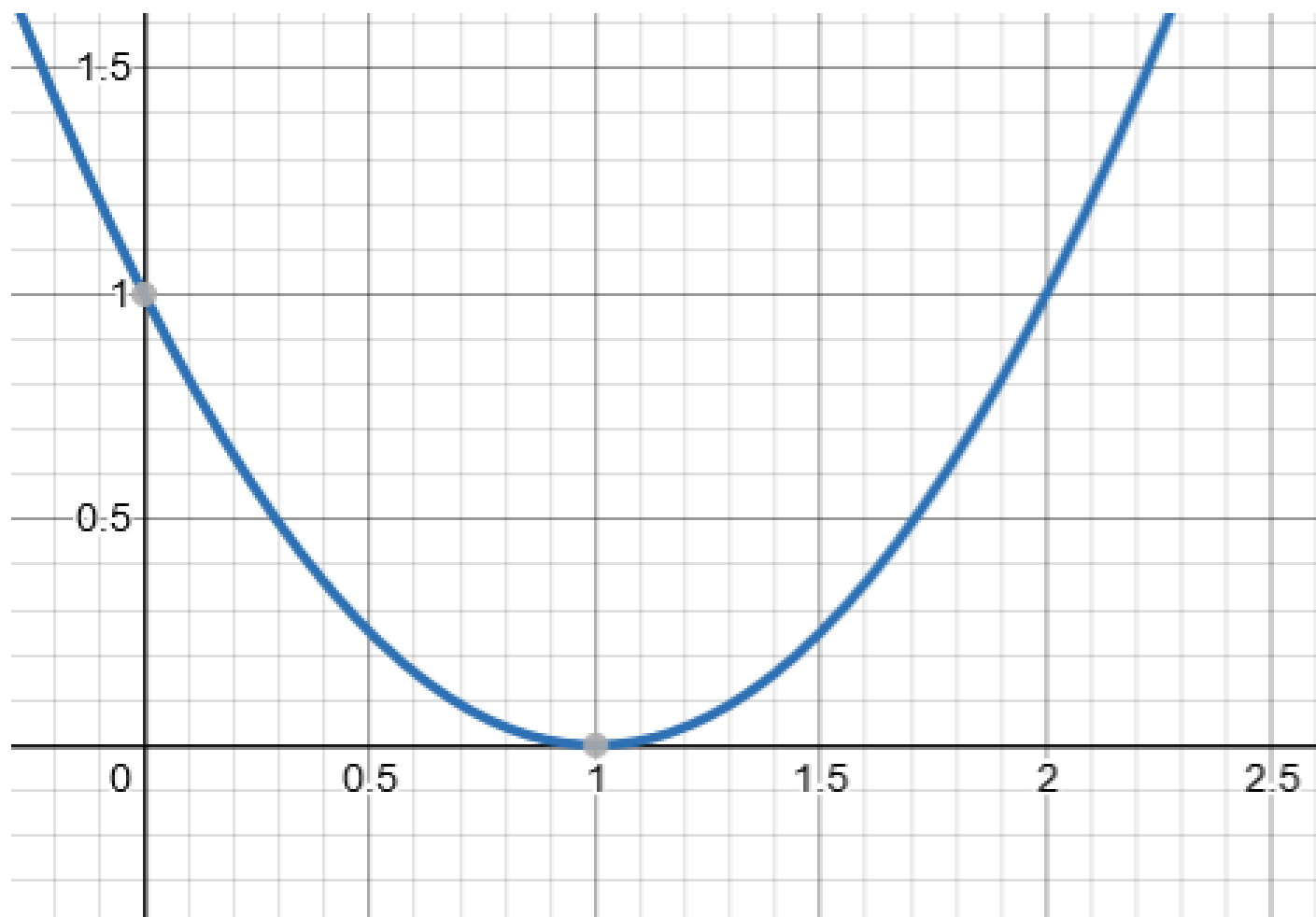


Ejemplos

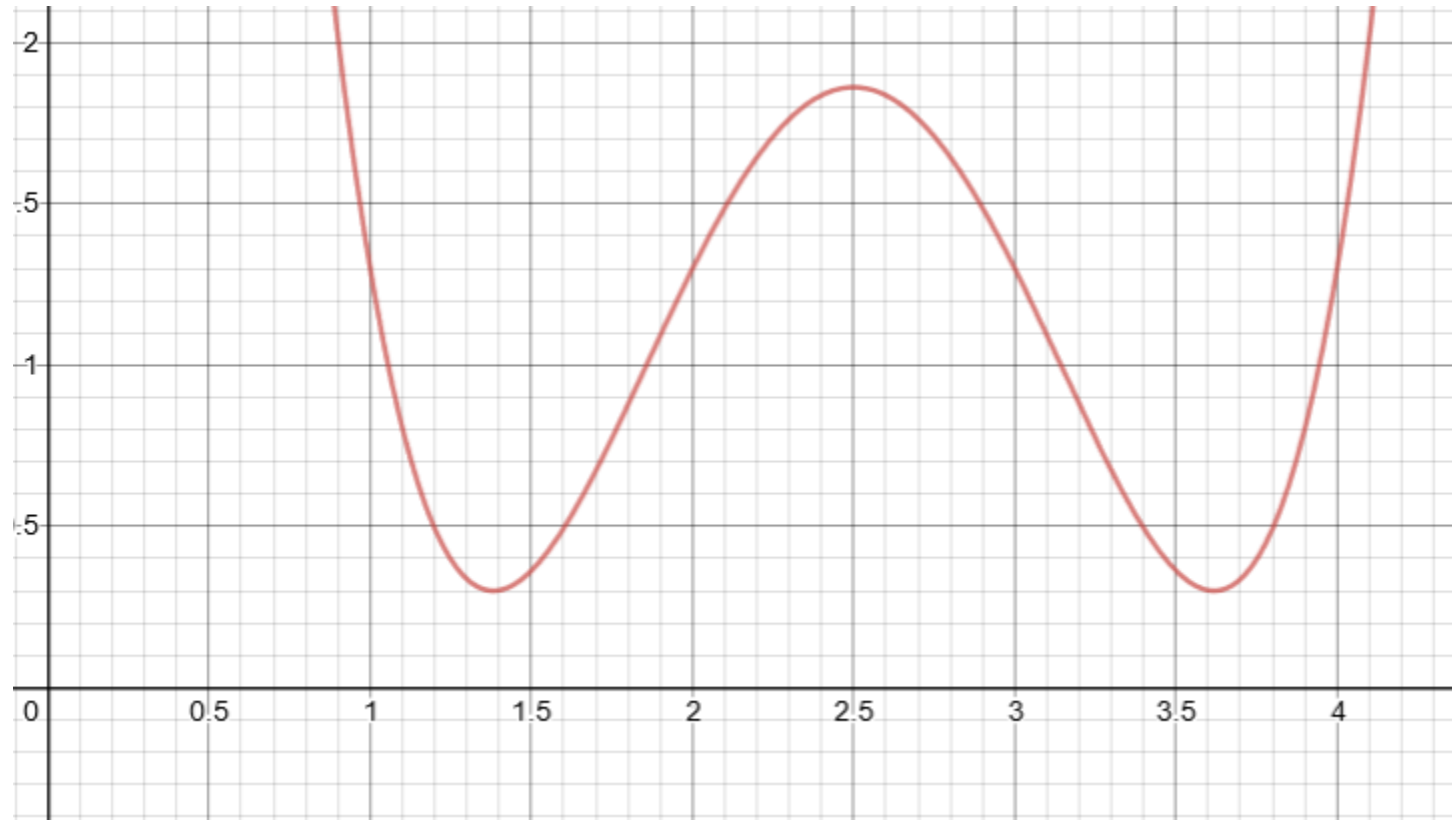
- $x^4 - 10x^3 + 35x^2 - 50x + 24 = (x - 1)(x - 2)(x - 3)(x - 4)$:



Las soluciones pueden ser iguales



Las soluciones pueden ser irracionales



Por eso tomamos el mejor caso

- $p(x_1)$ es de grado k
- Todas las k soluciones de $p(x_1)$ son distintas
- Todas las k soluciones de $p(x_1)$ están en $\mathbb{Q}$
- Todas las k soluciones de $p(x_1)$ están en A
- $k \leq |A|$
- a_1 se elije uniformemente en A
- La probabilidad de que a_1 sea solución de $p(x_1)$ es $\frac{k}{|A|}$

$$\Pr(p(a_1) = 0) = \frac{k}{|A|}$$

En casos peores

- Algunas o todas las k soluciones de $p(x_1)$ son iguales
- Algunas o todas las k soluciones de $p(x_1)$ no están en $\mathbb{Q}$
- Algunas o todas las k soluciones de $p(x_1)$ no están en A
- Entonces para todo caso:

$$\Pr(p(a_1) = 0) \leq \frac{k}{|A|}$$

Aclaración sobre el grado en varias variables

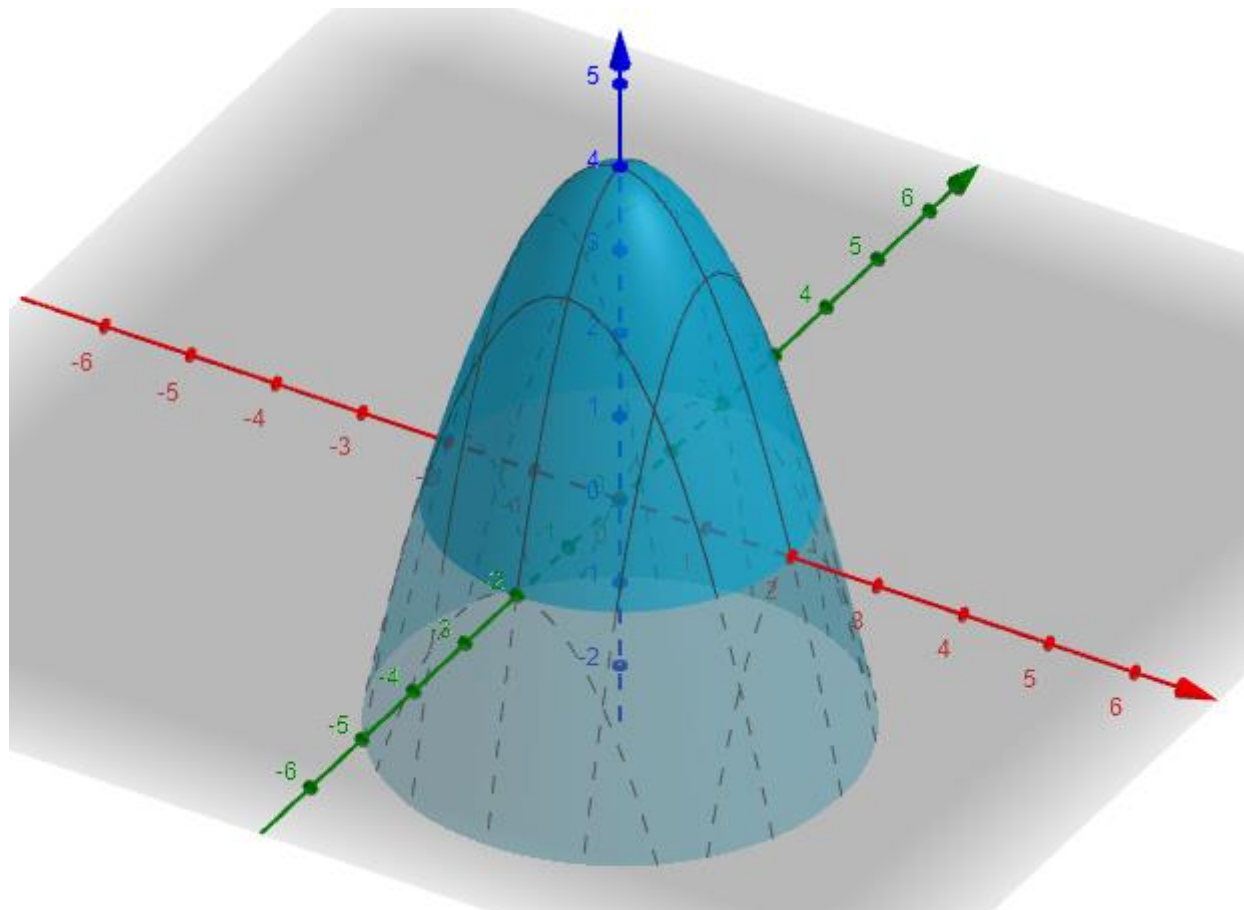
- Es el elemento cuya suma de exponentes es más alta
- $x + y + z + w$, $k = 1$
- $4 - x^2 - y^2$, $k = 2$
- $4 - x^2$, $k = 2$
- $4 - x^2y$, $k = 3$
- $-x^2yz$, $k = 4$

Para más de una variable

- Pueden haber infinitas soluciones

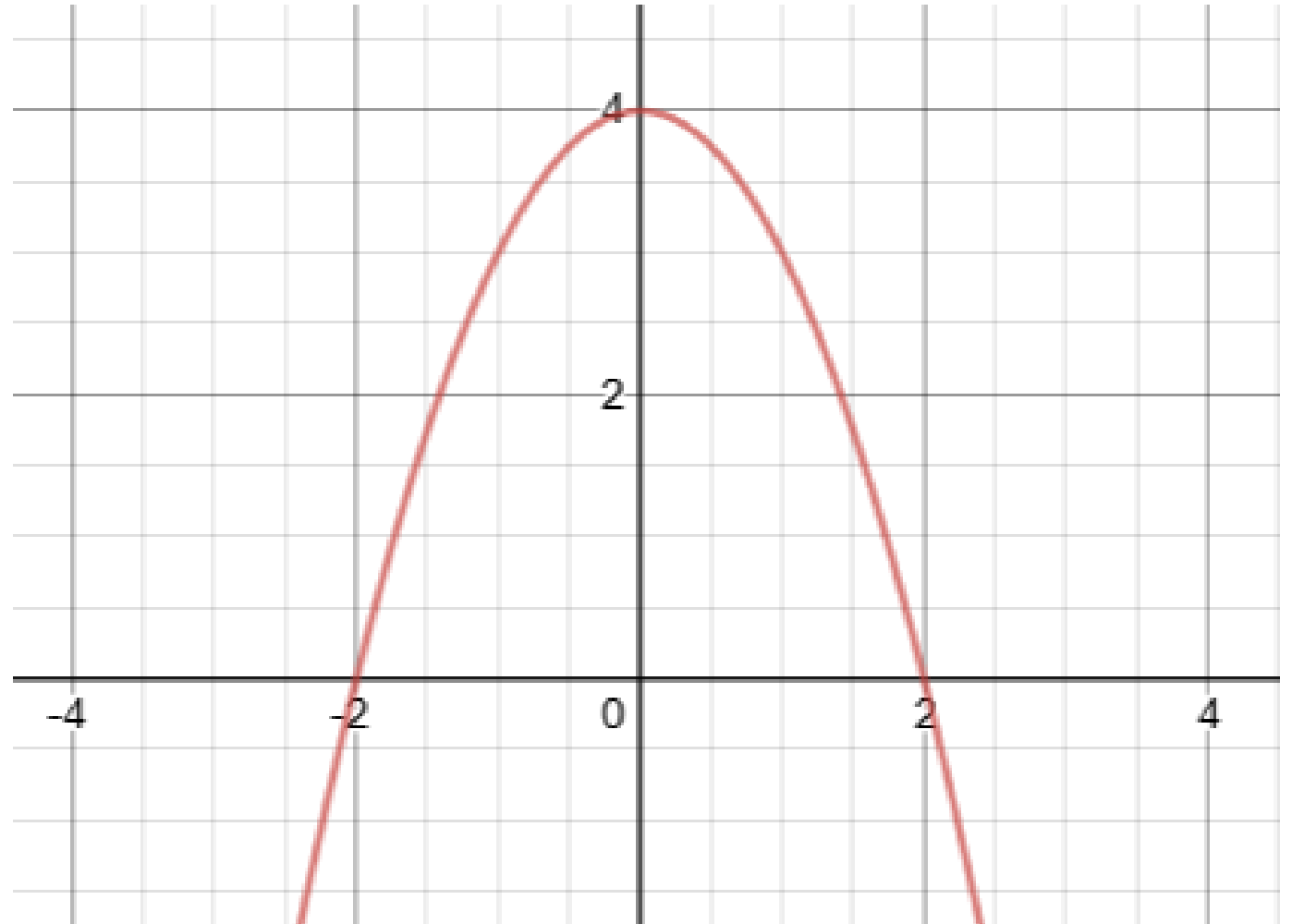
Ejemplo

- $4 - x^2 - y^2$



Al seleccionar una variable es hacer un corte

- $4 - x^2 - y^2$
- $y = 0$
- Da como resultado: $4 - x^2$



Solución

- Ordenamos las entradas del polinomio $p(x_1, \dots, x_n)$ segun su exponente más alto dentro del polinomio. En orden segun del exponente más bajo al más alto, en caso de igual exponente no importa el orden.
- Ejemplo:

$$p(w, x, y, z) = 4 - w^4 - x^3 - y^2 - z$$

$$p(z, y, x, w) = 4 - w^4 - x^3 - y^2 - z$$

Solución

- Seleccionamos uniformemente $a_1, \dots, a_{n-1}$

- Queda un polinomio de una sola variable:

$$p'(x_n) = p(a_1, \dots, a_{n-1}, x_n)$$

- Ejemplo:

$$p(z, y, x, w) = 4 - w^4 - x^3 - y^2 - z$$

$$p'(w) = p(a_1, a_2, a_3, w) = -w^4 + (4 - a_3^3 - a_2^2 - a_1)$$

Solución

- Hay un total de $|A|^{n-1}$ de estos posibles polinomios
- $p'(x_n)$ es de grado k_n , que es el exponente más alto en el polinomio original

- Ejemplo:

$$p'(w) = p(a_1, a_2, a_3, w) = -w^4 + (4 - a_3^3 - a_2^2 - a_1)$$
$$k_w = 4$$

El mayor caso para un $p'(x_n)$

- $p'(x_n)$ es no nulo
- Todas las soluciones de $p'(x_n)$ son diferentes
- Todas las soluciones de $p'(x_n)$ están en $\mathbb{Q}$
- Todas las soluciones de $p'(x_n)$ están en A
- La probabilidad es

$$\Pr(p'(a_n) = 0) = \frac{k_n}{|A|}$$

El mayor caso para todos los $|A|^{n-1}$ posibles $p'(x_n)$

- Todos los $p'(x_n)$ son no nulos
- Todas las soluciones de todos los posibles $p'(x_n)$ son diferentes
- Todas las soluciones de todos los posibles $p'(x_n)$ están en $\mathbb{Q}$
- Todas las soluciones de todos los posibles $p'(x_n)$ están en A
- La probabilidad es

$$\Pr(p(a_1, \dots, a_n) = 0) = |A| \left(\frac{1}{|A|} \dots \left(|A| \left(\frac{1}{|A|} \frac{k_n}{|A|} \right) \right) \right) = \frac{k_n}{|A|}$$

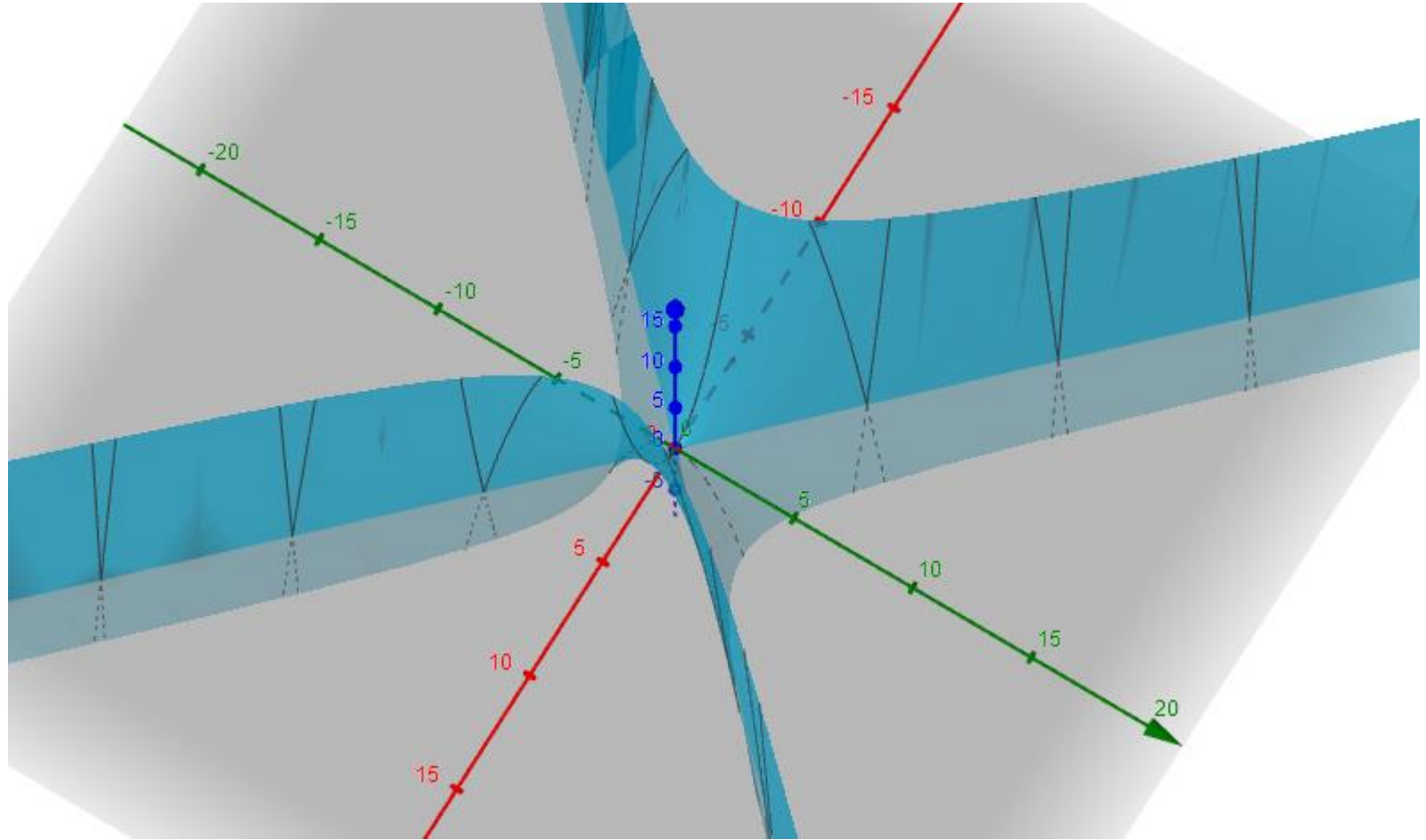
El mayor caso para $p(x_1, \dots, x_n)$

- $k_n = k$

$$\Pr(p(a_1, \dots, a_n) = 0) = \frac{k}{|A|}$$

Ejemplo simple

- $p(x, y) = x^2 - y^2$
- $k = 2$
- $A = \{-2, -1, 1, 2\}$
- $|A| = 4$



Ejemplo simple: casos

- Para $x = -2$
- $p(-2, y) = 4 - y^2$
- $\Pr(p(-2, a_2) = 0) = \Pr(a_2 = -2 \vee a_2 = 2) = \frac{2}{4}$

Ejemplo simple: casos

- Para $x = -1$
- $p(-1, y) = 1 - y^2$
- $\Pr(p(-1, a_2) = 0) = \Pr(a_2 = -1 \vee a_2 = 1) = \frac{2}{4}$

Ejemplo simple: casos

- Para $x = 1$
- $p(1, y) = 1 - y^2$
- $\Pr(p(1, a_2) = 0) = \Pr(a_2 = -1 \vee a_2 = 1) = \frac{2}{4}$

Ejemplo simple: casos

- Para $x = 2$
- $p(2, y) = 4 - y^2$
- $\Pr(p(2, a_2) = 0) = \Pr(a_2 = -2 \vee a_2 = 2) = \frac{2}{4}$

Ejemplo simple:casos

$$\frac{1}{4} \binom{2}{\frac{2}{4}} + \frac{1}{4} \binom{2}{\frac{2}{4}} + \frac{1}{4} \binom{2}{\frac{2}{4}} + \frac{1}{4} \binom{2}{\frac{2}{4}} = \frac{2}{4} = \frac{k}{|A|}$$

En casos peores

$$\Pr(p(a_1, \dots, a_n) = 0) \leq \frac{k}{|A|}$$