Introducción al principio local-global

Héctor Pastén

PUC Chile

21 de Agosto de 2018

Repaso: p-ádicos

Sea p primo. Los números p-ádicos $\mathbb{Q}_p$ y los enteros p-ádicos $\mathbb{Z}_p$ se pueden definir de dos formas equivalentes:

- *Analítica.* Usando $|-|_p$, la completación de $\mathbb{Q}$ es $\mathbb{Q}_p$. Entonces $\mathbb{Z}_p = \{x \in \mathbb{Q}_p : |x|_p \leq 1\}$. Además $\mathbb{Z} \subseteq \mathbb{Z}_p$ es denso.

Repaso: p-ádicos

Sea p primo. Los números p-ádicos $\mathbb{Q}_p$ y los enteros p-ádicos $\mathbb{Z}_p$ se pueden definir de dos formas equivalentes:

- *Analítica.* Usando $|-|_p$, la completación de $\mathbb{Q}$ es $\mathbb{Q}_p$. Entonces $\mathbb{Z}_p = \{x \in \mathbb{Q}_p : |x|_p \leq 1\}$. Además $\mathbb{Z} \subseteq \mathbb{Z}_p$ es denso.
- *Algebraica.* $\mathbb{Z}_p$ es el límite proyectivo

$$\mathbb{Z}_p = \text{lím}\left(\mathbb{Z}/p\mathbb{Z} \leftarrow \mathbb{Z}/p^2\mathbb{Z} \leftarrow \ldots\right) = \{\text{secuencias compatibles}\}.$$

$\mathbb{Z} \simeq \{(n \mod p^r)_{r\geq 1} : n \in \mathbb{Z}\} \subseteq \mathbb{Z}_p$. Además $\mathbb{Z}_p$ es un dominio entero y $\mathbb{Q}_p$ es su campo de fracciones.

Repaso: p-ádicos

Sea p primo. Los números p-ádicos $\mathbb{Q}_p$ y los enteros p-ádicos $\mathbb{Z}_p$ se pueden definir de dos formas equivalentes:

- *Analítica.* Usando $|-|_p$, la completación de $\mathbb{Q}$ es $\mathbb{Q}_p$. Entonces $\mathbb{Z}_p = \{x \in \mathbb{Q}_p : |x|_p \leq 1\}$. Además $\mathbb{Z} \subseteq \mathbb{Z}_p$ es denso.
- *Algebraica.* $\mathbb{Z}_p$ es el límite proyectivo

$$\mathbb{Z}_p = \text{lím}\left(\mathbb{Z}/p\mathbb{Z} \leftarrow \mathbb{Z}/p^2\mathbb{Z} \leftarrow ...\right) = \{\text{secuencias compatibles}\}.$$

$\mathbb{Z} \simeq \{(n \mod p^r)_{r\geq 1} : n \in \mathbb{Z}\} \subseteq \mathbb{Z}_p$. Además $\mathbb{Z}_p$ es un dominio entero y $\mathbb{Q}_p$ es su campo de fracciones.

En ambos casos, los elementos de $\mathbb{Z}_p$ se pueden escribir en la forma

$$x = a_0 + a_1 p + a_2 p^2 + ... = (...a_2 a_1 a_0)_p\,; \quad a_j \in \{0, 1, ..., p-1\}.$$

Repaso: p-ádicos

Ejemplo. $p = 2$. Consideramos el número 2-ádico

$$x = \ldots 111_2 = 1 + 2 + 4 + 8 + \ldots \in \mathbb{Z}_2.$$

Veamos que $x = -1$.

Repaso: p-ádicos

Ejemplo. $p = 2$. Consideramos el número 2-ádico

$$x = \ldots 111_2 = 1 + 2 + 4 + 8 + \ldots \in \mathbb{Z}_2.$$

Veamos que $x = -1$.

- *Analítica.* Es la serie geométrica

$$1 + \gamma + \gamma^2 + \ldots \quad \text{con } \gamma = 2 \text{ y } |\gamma|_2 = |2|_2 = 1/2 < 1$$

así que converge en $\mathbb{Q}_2$. Su suma es $1/(1-\gamma) = 1/(1-2) = -1$.

Repaso: p-ádicos

Ejemplo. $p = 2$. Consideramos el número 2-ádico

$$x = \ldots 111_2 = 1 + 2 + 4 + 8 + \ldots \in \mathbb{Z}_2.$$

Veamos que $x = -1$.

- *Analítica.* Es la serie geométrica

$$1 + \gamma + \gamma^2 + \ldots \quad \text{con } \gamma = 2 \text{ y } |\gamma|_2 = |2|_2 = 1/2 < 1$$

así que converge en $\mathbb{Q}_2$. Su suma es $1/(1-\gamma) = 1/(1-2) = -1$.

- *Algebraica.* Para cada $r \geq 1$ tenemos

$$1 + x \equiv 1 + (1 + 2 + \ldots + 2^{r-1}) \equiv 0 \mod 2^r \Rightarrow x \equiv -1 \mod 2^r$$

así que x es la secuencia compatible $(-1 \mod 2^r)_r \in \mathbb{Z}_2$.

Repaso: p-ádicos

Recordamos también el Lema de Hensel.

Teorema (Lema de Hensel)

Sea $f(t) \in \mathbb{Z}_p[t]$ polinomio y sea $a \in \mathbb{Z}_p$. Suponga que

$$|f(a)|_p < |f'(a)|_p^2.$$

Entonces existe un único $b \in \mathbb{Z}_p$ tal que

(i) $f(b) = 0$, *y*

(ii) $|a - b|_p < |f'(a)|_p$.

Repaso: p-ádicos

Ejemplo. Veamos que $x^2 + x + 25 = 0$ tiene solución en $\mathbb{Z}_3$.

- Tomar $f(t) = t^2 + t + 25$, $a = 1$. Notar que $f'(t) = 2t + 1$.
- $f(a) = 27, f'(a) = 3 \Longrightarrow |f(a)|_3 = 1/27 < 1/9 = |f'(a)|_3^2$.

Por lo tanto existe solución $b \in \mathbb{Z}_3$.

Repaso: p-ádicos

Ejemplo. Veamos que $x^2 + x + 25 = 0$ tiene solución en $\mathbb{Z}_3$.

- Tomar $f(t) = t^2 + t + 25$, $a = 1$. Notar que $f'(t) = 2t + 1$.
- $f(a) = 27, f'(a) = 3 \Longrightarrow |f(a)|_3 = 1/27 < 1/9 = |f'(a)|_3^2$.

Por lo tanto existe solución $b \in \mathbb{Z}_3$.
La demostración del lema del Hensel es constructiva: ¡es el método de Newton-Raphson! En este ejemplo tomando $x_0 = a = \ldots 001_3$ se obtiene

$$\begin{aligned} x_1 &= x_0 - f(x_0)/f'(x_0) = 1 - 27/3 = -8 = 1 + 9 \cdot (-1) \\ &= 1 + 9 \cdot (2 + 2 \cdot 3 + 2 \cdot 9 + \ldots) = \ldots 22201_3 \end{aligned}$$

Observe que $f(x_1)$ es mejor aproximación de 0 que $f(x_0)$:

$$\begin{aligned} x_0^2 + x_0 + 25 = f(1) = 27 \quad &= \ldots 001000_3 \\ x_1^2 + x_1 + 25 = f(-8) = 81 \quad &= \ldots 010000_3 \end{aligned}$$

Soluciones locales

Veamos si hay soluciones enteras para las ecuaciones

$$(i)\, x^2 - 6y^2 - 1 = 0, \quad (ii)\, x^2 - 6y^2 + 1 = 0, \quad (iii)\, x^2 + 6y^2 + 1 = 0.$$

Soluciones locales

Veamos si hay soluciones enteras para las ecuaciones

$$(i)\, x^2 - 6y^2 - 1 = 0, \quad (ii)\, x^2 - 6y^2 + 1 = 0, \quad (iii)\, x^2 + 6y^2 + 1 = 0.$$

(i) Sí. Algunas soluciones son $(1, 0)$, $(5, 2)$, $(49, 20)$.

Soluciones locales

Veamos si hay soluciones enteras para las ecuaciones

$$(i)\, x^2 - 6y^2 - 1 = 0, \quad (ii)\, x^2 - 6y^2 + 1 = 0, \quad (iii)\, x^2 + 6y^2 + 1 = 0.$$

(i) Sí. Algunas soluciones son $(1, 0)$, $(5, 2)$, $(49, 20)$.

(ii) No. Esa ecuación ni siquiera se puede resolver módulo 8. Los cuadrados en $\mathbb{Z}/8\mathbb{Z}$ son $0, 1, 4$ así que $x^2 \equiv 0, 1, 4 \mod 8$ y $-6y^2 \equiv 0, 2 \mod 8$. No suman $-1 \mod 8$.

Soluciones locales

Veamos si hay soluciones enteras para las ecuaciones

$$(i)\, x^2 - 6y^2 - 1 = 0, \quad (ii)\, x^2 - 6y^2 + 1 = 0, \quad (iii)\, x^2 + 6y^2 + 1 = 0.$$

(i) Sí. Algunas soluciones son $(1, 0)$, $(5, 2)$, $(49, 20)$.

(ii) No. Esa ecuación ni siquiera se puede resolver módulo 8. Los cuadrados en $\mathbb{Z}/8\mathbb{Z}$ son $0, 1, 4$ así que $x^2 \equiv 0, 1, 4 \mod 8$ y $-6y^2 \equiv 0, 2 \mod 8$. No suman $-1 \mod 8$.

(iii) No. Esa ecuación ni siquiera se puede resolver en $\mathbb{R}$!

Soluciones locales

Veamos si hay soluciones enteras para las ecuaciones

$$(i)\, x^2 - 6y^2 - 1 = 0, \quad (ii)\, x^2 - 6y^2 + 1 = 0, \quad (iii)\, x^2 + 6y^2 + 1 = 0.$$

(i) Sí. Algunas soluciones son $(1, 0)$, $(5, 2)$, $(49, 20)$.

(ii) No. Esa ecuación ni siquiera se puede resolver módulo 8. Los cuadrados en $\mathbb{Z}/8\mathbb{Z}$ son $0, 1, 4$ así que $x^2 \equiv 0, 1, 4 \mod 8$ y $-6y^2 \equiv 0, 2 \mod 8$. No suman $-1 \mod 8$.

(iii) No. Esa ecuación ni siquiera se puede resolver en $\mathbb{R}$!

En el caso (ii) no bastaba trabajar en $\mathbb{Z}/2\mathbb{Z}$ o $\mathbb{Z}/4\mathbb{Z}$. Fue necesario trabajar con $\mathbb{Z}/2^r\mathbb{Z}$ para $r = 1, 2, 3, \ldots$ es decir, 2-ádicamente.

Soluciones locales

Teorema (Criterio local)

Sea $F \in \mathbb{Z}[x_1, ..., x_k]$. Si la ecuación diofantina

$$F(x_1, ..., x_k) = 0$$

tiene soluciones en $\mathbb{Z}$, entonces tiene soluciones en $\mathbb{R}$ y en $\mathbb{Z}_p$ para todo p. Dicho de otra forma, para mostrar que $F = 0$ no tiene soluciones enteras, basta que no tenga soluciones en $\mathbb{R}$ o en $\mathbb{Z}_p$ para algún primo p.

Variaciones:

- Para F homogéneo se excluye la solución trivial $(0, 0, ..., 0)$.
- También se pueden considerar sistemas de ecuaciones.
- También se puede trabajar con $\mathbb{Q}$ y $\mathbb{Q}_p$ en lugar de $\mathbb{Z}$ y $\mathbb{Z}_p$.

El criterio local no siempre es suficiente

Veamos el ejemplo $x^2 + 11y^2 = 3$

- *No hay solución en* $\mathbb{Z}$. Evidente, por agotamiento de casos.

El criterio local no siempre es suficiente

Veamos el ejemplo $x^2 + 11y^2 = 3$

- *No hay solución en* $\mathbb{Z}$. Evidente, por agotamiento de casos.
- *Hay solución en* $\mathbb{R}$. Por ejemplo $(\sqrt{3}, 0)$.

El criterio local no siempre es suficiente

Veamos el ejemplo $x^2 + 11y^2 = 3$

- *No hay solución en* $\mathbb{Z}$. Evidente, por agotamiento de casos.
- *Hay solución en* $\mathbb{R}$. Por ejemplo $(\sqrt{3}, 0)$.
- *Hay solución en* $\mathbb{Z}_2$. Aplicamos el lema de Hensel con $f(t) = 11t^2 - 3$ y $a = 1$. Tenemos

$$|f'(a)|_2 = |22 \cdot 1|_2 = 1/2 \Rightarrow |f(a)|_2 = |8|_2 = 1/8 < |f'(a)|_2^2$$

así que existe $b \in \mathbb{Z}_2$ con $11b^2 = 3$. Tomar $(x, y) = (0, b)$.

El criterio local no siempre es suficiente

Veamos el ejemplo $x^2 + 11y^2 = 3$

- *No hay solución en* $\mathbb{Z}$. Evidente, por agotamiento de casos.
- *Hay solución en* $\mathbb{R}$. Por ejemplo $(\sqrt{3}, 0)$.
- *Hay solución en* $\mathbb{Z}_2$. Aplicamos el lema de Hensel con $f(t) = 11t^2 - 3$ y $a = 1$. Tenemos

$$|f'(a)|_2 = |22 \cdot 1|_2 = 1/2 \Rightarrow |f(a)|_2 = |8|_2 = 1/8 < |f'(a)|_2^2$$

así que existe $b \in \mathbb{Z}_2$ con $11b^2 = 3$. Tomar $(x, y) = (0, b)$.

- *Hay solución en* $\mathbb{Z}_{11}$. Ejercicio. Similar al caso $p = 2$, pero tomando $f(t) = t^2$ y $a = 5$. Entonces la solución será $(x, y) = (b, 0)$.

El criterio local no siempre es suficiente

Veamos el ejemplo $x^2 + 11y^2 = 3$

- *No hay solución en* $\mathbb{Z}$. Evidente, por agotamiento de casos.
- *Hay solución en* $\mathbb{R}$. Por ejemplo $(\sqrt{3}, 0)$.
- *Hay solución en* $\mathbb{Z}_2$. Aplicamos el lema de Hensel con $f(t) = 11t^2 - 3$ y $a = 1$. Tenemos

$$|f'(a)|_2 = |22 \cdot 1|_2 = 1/2 \Rightarrow |f(a)|_2 = |8|_2 = 1/8 < |f'(a)|_2^2$$

  así que existe $b \in \mathbb{Z}_2$ con $11b^2 = 3$. Tomar $(x, y) = (0, b)$.
- *Hay solución en* $\mathbb{Z}_{11}$. Ejercicio. Similar al caso $p = 2$, pero tomando $f(t) = t^2$ y $a = 5$. Entonces la solución será $(x, y) = (b, 0)$.
- *Hay solución en* $\mathbb{Z}_p$ *para todo* $p \neq 2, 11$. También por Hensel.

El criterio local no siempre es suficiente

$$x^2 + 11y^2 = 3$$

No hay solución en $\mathbb{Z}$. Listo.
Hay solución en $\mathbb{R}$, $\mathbb{Z}_2$ *y* $\mathbb{Z}_{11}$. Listo.
Hay solución en $\mathbb{Z}_p$ *para todo* $p \neq 2, 11$. Dos partes:

El criterio local no siempre es suficiente

$$x^2 + 11y^2 = 3$$

No hay solución en $\mathbb{Z}$. Listo.
Hay solución en $\mathbb{R}$, $\mathbb{Z}_2$ *y* $\mathbb{Z}_{11}$. Listo.
Hay solución en $\mathbb{Z}_p$ *para todo* $p \neq 2, 11$. Dos partes:

- *Hay solución módulo* p. Sea $C \subseteq \mathbb{Z}/p\mathbb{Z}$ el conjunto de cuadrados. Como $p > 2$ tenemos $\#C = (p+1)/2$. Los conjuntos $3 - C$ y $11 \cdot C$ también tienen $(p+1)/2$ elementos así que se intersectan.

El criterio local no siempre es suficiente

$$x^2 + 11y^2 = 3$$

No hay solución en $\mathbb{Z}$. Listo.
Hay solución en $\mathbb{R}$, $\mathbb{Z}_2$ *y* $\mathbb{Z}_{11}$. Listo.
Hay solución en $\mathbb{Z}_p$ *para todo* $p \neq 2, 11$. Dos partes:

- *Hay solución módulo* p. Sea $C \subseteq \mathbb{Z}/p\mathbb{Z}$ el conjunto de cuadrados. Como $p > 2$ tenemos $\#C = (p+1)/2$. Los conjuntos $3 - C$ y $11 \cdot C$ también tienen $(p+1)/2$ elementos así que se intersectan.
- *Levantar la solución a* $\mathbb{Z}_p$. Sea $(a_1, a_2) \in \mathbb{Z}^2$ una solución módulo p. No puede ser que $a_j \equiv 0 \mod p$ para ambos $j = 1, 2$. Digamos $a_1 \not\equiv 0 \mod p$ (el otro caso es similar). Defina $f(t) = t^2 + 11b^2 - 3$. La ecuación $f(t) = 0$ cumple las condiciones del lema de Hensel y obtenemos una solución $b \in \mathbb{Z}_p$. Tomar $(x, y) = (b, a_2)$.

El criterio local no siempre es suficiente

La ecuación

$$x^2 + 11x^2 = 3$$

no tiene soluciones en $\mathbb{Z}$ (global), pero tiene soluciones en todos los $\mathbb{Z}_p$ y en $\mathbb{R}$ (local). Así que el criterio local no era suficiente para detectar la inexistencia de soluciones enteras.

Para las ecuaciones diofantinas donde el criterio local *sí es suficiente*, diremos que **se cumple el principio local-global**. De otra forma, diremos que **el principio local-global falla**.

Un ejemplo donde se cumple el principio local-global

Proposición

El principio local-global se cumple para ecuaciones de la forma $x^2 = n$ con n entero impar.

En realidad no es necesario que n sea impar, pero en este caso la demostración es más sencilla.
La demostración usará tres herramientas que recordamos a continuación:

- Teorema Chino
- Teorema de Dirichlet
- Reciprocidad cuadrática.

Un ejemplo donde se cumple el principio local-global

Teorema (Teorema Chino)

Si $m_1, ..., m_r$ son coprimos de a pares, entonces tenemos el un isomorfismo de anillos

$$\psi : \mathbb{Z}/(m_1 \cdots m_r)\mathbb{Z} \simeq \mathbb{Z}/m_1\mathbb{Z} \times ... \times \mathbb{Z}/m_r\mathbb{Z}$$
$$n \mod m_1 \cdots m_r \mapsto (n \mod m_1, ..., n \mod m_r)$$

Un ejemplo donde se cumple el principio local-global

Teorema (Teorema Chino)

Si $m_1, ..., m_r$ son coprimos de a pares, entonces tenemos el un isomorfismo de anillos

$$\begin{aligned}\psi :&\mathbb{Z}/(m_1 \cdots m_r)\mathbb{Z} \simeq \mathbb{Z}/m_1\mathbb{Z} \times ... \times \mathbb{Z}/m_r\mathbb{Z} \\ &n \mod m_1 \cdots m_r \mapsto (n \mod m_1, ..., n \mod m_r)\end{aligned}$$

Ejemplo. $\mathbb{Z}/15\mathbb{Z} \simeq \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}$. Así, el sistema de congruencias

$$\begin{cases} x \equiv 2 \mod 3 \\ x \equiv 4 \mod 5 \end{cases}$$

es equivalente a la congruencia $x \equiv 14 \mod 15$, porque

$$\psi(14\,(15)) = (14\,(3), 14\,(5)) = (2\,(3), 4\,(5)).$$

Un ejemplo donde se cumple el principio local-global

Teorema (Dirichlet; primos en una progresión aritmética)

Sea $N > 1$ entero y sea a coprimo con N. Existen infinitos primos p que cumplen $p \equiv a \mod N$.

Un ejemplo donde se cumple el principio local-global

Teorema (Dirichlet; primos en una progresión aritmética)

Sea $N > 1$ entero y sea a coprimo con N. Existen infinitos primos p que cumplen $p \equiv a \mod N$.

Ejemplo. Como $\gcd(3, 10) = 1$, hay infinitos primos $p \equiv 3 \mod 10$. Por lo tanto, hay infinitos primos cuyo último dígito es 3.

$$\boxed{3}, \boxed{13}, \boxed{23}, 33, \boxed{43}, \boxed{53}, 63, \boxed{73}, \boxed{83}, 93, \boxed{103},$$
$$\boxed{113}, 123, 133, 143, 153, \boxed{163}, \boxed{173}, 183, \boxed{193}, \ldots$$

Un ejemplo donde se cumple el principio local-global

Sea $p > 2$ primo. Para un entero N defina el símbolo de Legendre

$$(N/p) = \begin{cases} 0 & \text{si } N \equiv 0 \mod p \\ 1 & \text{si } N \not\equiv 0 \mod p \text{ y es residuo cuadrático} \\ -1 & \text{si } N \not\equiv 0 \mod p \text{ y no es residuo cuadrático} \end{cases}$$

La función $(-/p)$ es completamente multiplicativa.

Un ejemplo donde se cumple el principio local-global

Sea $p > 2$ primo. Para un entero N defina el símbolo de Legendre

$$(N/p) = \begin{cases} 0 & \text{si } N \equiv 0 \mod p \\ 1 & \text{si } N \not\equiv 0 \mod p \text{ y es residuo cuadrático} \\ -1 & \text{si } N \not\equiv 0 \mod p \text{ y no es residuo cuadrático} \end{cases}$$

La función $(-/p)$ es completamente multiplicativa.

Teorema (Reciprocidad cuadrática)

Si $p, q > 2$ son primos distintos, se tiene

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{(p-1)(q-1)/4}.$$

Un ejemplo donde se cumple el principio local-global

Teorema (Reciprocidad cuadrática)

Si $p, q > 2$ son primos distintos, se tiene

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{(p-1)(q-1)/4}.$$

Ejemplo.

$$\left(\frac{7}{61}\right) = (-1)^{6\cdot 60/4}\left(\frac{61}{7}\right) = \left(\frac{61}{7}\right) = \left(\frac{5}{7}\right) = -1$$

así que 7 no es un cuadrado módulo 61.

Un ejemplo donde se cumple el principio local-global

Ahora estamos listos para demostrar:

Proposición

El principio local-global se cumple para ecuaciones de la forma $x^2 = n$ con n entero impar.

Un ejemplo donde se cumple el principio local-global

Suponer que $x^2 = n$ no tiene solución en $\mathbb{Z}$ pero tiene en $\mathbb{Z}_p$ $(\forall p)$ y en $\mathbb{R}$.

Un ejemplo donde se cumple el principio local-global

Suponer que $x^2 = n$ no tiene solución en $\mathbb{Z}$ pero tiene en $\mathbb{Z}_p$ $(\forall p)$ y en $\mathbb{R}$.

- Solución en $\mathbb{R}$ implica que $n > 0$.
- Sin solución en $\mathbb{Z}$ implica $n = a^2 b$ donde $b > 1$ es libre de cuadrados.

La factorización de b es $b = q_1 \cdots q_r$ con $r \geq 1$ y los $q_j > 2$ primos distintos.

Un ejemplo donde se cumple el principio local-global

Suponer que $x^2 = n$ no tiene solución en $\mathbb{Z}$ pero tiene en $\mathbb{Z}_p$ $(\forall p)$ y en $\mathbb{R}$.

- Solución en $\mathbb{R}$ implica que $n > 0$.
- Sin solución en $\mathbb{Z}$ implica $n = a^2 b$ donde $b > 1$ es libre de cuadrados.

La factorización de b es $b = q_1 \cdots q_r$ con $r \geq 1$ y los $q_j > 2$ primos distintos.
Sea $p > 2$ un primo y vamos a pedir las siguientes condiciones:

(i) $p \equiv 1\,(4)$. Así, para todo primo $q > 2$ se tiene $(q/p) = (p/q)$.

(ii) $p \equiv c\,(q_1)$ con c no-cuadrado en $\mathbb{Z}/q_1\mathbb{Z}$. Así, $(p/q_1) = -1$.

(iii) $p \equiv 1\,(q_j)$ para todo $j > 1$. Esto implica $(p/q_j) = 1$ para todo $j > 1$.

(iv) $p > n$, lo que implica $p \nmid n$.

Teorema Chino y teorema de Dirichlet implican que p existe.

Un ejemplo donde se cumple el principio local-global

Suponer que $x^2 = n$ no tiene solución en $\mathbb{Z}$ pero tiene en $\mathbb{Z}_p$ $(\forall p)$ y en $\mathbb{R}$.

- Solución en $\mathbb{R}$ implica que $n > 0$.
- Sin solución en $\mathbb{Z}$ implica $n = a^2 b$ donde $b > 1$ es libre de cuadrados.

La factorización de b es $b = q_1 \cdots q_r$ con $r \geq 1$ y los $q_j > 2$ primos distintos.
Sea $p > 2$ un primo y vamos a pedir las siguientes condiciones:

(i) $p \equiv 1\,(4)$. Así, para todo primo $q > 2$ se tiene $(q/p) = (p/q)$.

(ii) $p \equiv c\,(q_1)$ con c no-cuadrado en $\mathbb{Z}/q_1\mathbb{Z}$. Así, $(p/q_1) = -1$.

(iii) $p \equiv 1\,(q_j)$ para todo $j > 1$. Esto implica $(p/q_j) = 1$ para todo $j > 1$.

(iv) $p > n$, lo que implica $p \nmid n$.

Teorema Chino y teorema de Dirichlet implican que p existe. Finalmente:

$$1 = \left(\frac{n}{p}\right) = \left(\frac{a^2 b}{p}\right) = \left(\frac{b}{p}\right) = \prod_{j=1}^{r} \left(\frac{q_j}{p}\right) = \prod_{j=1}^{r} \left(\frac{p}{q_j}\right) = (-1) \cdot 1 \cdots 1 = -1. \,(!)$$

Un ejemplo importante

Teorema

El principio local-global se cumple para soluciones no-triviales de ecuaciones homogéneas de segundo grado.

"no-trivial" significa que excluimos la solución $(0, ..., 0)$.
Por ejemplo, una ecuación de la forma

$$ax^2 + by^2 + cz^2 = 0$$

con $a, b, c \in \mathbb{Z}$ tiene una solución entera no-trivial si y solo si tiene solución no-trivial en $\mathbb{R}$ y en $\mathbb{Z}_p$ para cada primo p. Sin embargo...

Un ejemplo importante

Teorema

El principio local-global se cumple para soluciones no-triviales de ecuaciones homogéneas de segundo grado.

"no-trivial" significa que excluimos la solución $(0, ..., 0)$.
Por ejemplo, una ecuación de la forma

$$ax^2 + by^2 + cz^2 = 0$$

con $a, b, c \in \mathbb{Z}$ tiene una solución entera no-trivial si y solo si tiene solución no-trivial en $\mathbb{R}$ y en $\mathbb{Z}_p$ para cada primo p. Sin embargo...

Ejemplo (Selmer, 1951)

La ecuación $3x^3 + 4y^3 + 5z^3 = 0$ *no tiene soluciones no-triviales en* $\mathbb{Z}$, *pero sí tiene en* $\mathbb{R}$ *y en cada* $\mathbb{Z}_p$.

Fin.