

El teorema de los cuatro cuadrados y el teorema de Minkowski

Alexey Beshenov (cadadr@gmail.com)

Universidad de El Salvador. Marzo de 2018

Uno de los primeros teóricos de números europeos fue el matemático francés Claude Gaspard Bachet de Méziriac (1581–1638). En 1621 Bachet publicó la traducción en latín de la *Arithmetica* de Diofanto. En sus notas Bachet mencionó la siguiente conjetaura.

Cada entero $n \geq 0$ puede expresarse como la suma de cuatro cuadrados:

$$n = a^2 + b^2 + c^2 + d^2, \quad a, b, c, d \in \mathbb{Z}.$$

Por ejemplo,

$$\begin{aligned} 7 &= 2^2 + 1^2 + 1^2 + 1^2, \\ 15 &= 3^2 + 2^2 + 1^2 + 1^2, \\ 28 &= 3^2 + 3^2 + 3^2 + 1^2. \end{aligned}$$

La primera demostración de esta conjetaura fue obtenida por Lagrange en 1770. En esta nota voy a presentar una demostración basada en el teorema de Minkowski sobre los conjuntos convexos simétricos. Es un resultado más reciente, probado por Hermann Minkowski en 1889, pero es de mucha importancia en aritmética y vale la pena revisarlo.

1 Cuaterniones y la identidad de los cuatro cuadrados de Euler

Los **cuaterniones** fueron introducidos en 1843 por el matemático irlandés William Rowan Hamilton (1805–1865). Hamilton estaba muy orgulloso de su descubrimiento y hasta escribió un libro de más de 800 páginas sobre el tema, que fue publicado póstumamente. Por falta de tiempo y entusiasmo, voy a revisar solamente un par de resultados necesarios. A cuatro números reales $a, b, c, d \in \mathbb{R}$ podemos asociar la matriz compleja de 2×2

$$\begin{pmatrix} a+bi & c+di \\ -c+di & a-bi \end{pmatrix}.$$

Esencialmente, es un cuaternion. Un cálculo tedioso nos da la expresión para el producto de dos cuaterniones. Es de la misma forma:

$$\begin{aligned} &\begin{pmatrix} a+bi & c+di \\ -c+di & a-bi \end{pmatrix} \cdot \begin{pmatrix} x+yi & z+wi \\ -z+wi & x-yi \end{pmatrix} \\ &= \begin{pmatrix} +(ax - by - cz - dw) + (ay + bx + cw - dz)i & +(az - bw + cx + dy) + (aw + bz - cy + dx)i \\ -(az - bw + cx + dy) + (aw + bz - cy + dx)i & +(ax - by - cz - dw) - (ay + bx + cw - dz)i \end{pmatrix}. \end{aligned}$$

La **norma** de un cuaternión es el determinante de la matriz correspondiente:

$$\det \begin{pmatrix} a+bi & c+di \\ -c+di & a-bi \end{pmatrix} = (a+bi)(a-bi) - (c+di)(-c+di) = a^2 + b^2 + c^2 + d^2.$$

El determinante de matrices es multiplicativo: tenemos $\det(AB) = \det(A) \cdot \det(B)$. En nuestro caso, comparando las últimas dos expresiones, se obtiene

$$(a^2 + b^2 + c^2 + d^2) \cdot (x^2 + y^2 + z^2 + w^2) \\ = (ax - by - cz - dw)^2 + (ay + bx + cw - dz)^2 + (az - bw + cx + dy)^2 + (aw + bz - cy + dx)^2.$$

Esta fórmula se conoce como la **identidad de los cuatro cuadrados de Euler** y apareció por primera vez en una carta de Euler a Goldbach de 1749. De hecho, la identidad de Euler no tiene nada que ver con los cuaterniones (que todavía no habían sido descubiertos) y se cumple en cualquier anillo comutativo, como se puede comprobar desarrollando las expresiones. Sin embargo, tal prueba explica aún menos que nuestra prueba con cuaterniones.

Euler necesitaba su identidad para el siguiente resultado.

Lema. *Si dos enteros $m, n \geq 0$ son sumas de cuatro cuadrados, entonces mn es también una suma de cuatro cuadrados.*

Esto significa en particular que para demostrar el teorema de los cuatro cuadrados, sería suficiente demostrarlo para todos los números primos. Por ejemplo, tenemos

$$2 = 1^2 + 1^2, \\ 3 = 1^2 + 1^2 + 1^2, \\ 5 = 2^2 + 1^2,$$

y con ayuda de la identidad de Euler se puede obtener la expresión

$$30 = 4^2 + 3^2 + 2^2 + 1^2.$$

Entonces, a partir de ahora, podemos enfocarnos en búsqueda de las expresiones

$$p = a^2 + b^2 + c^2 + d^2$$

para p primo y $a, b, c, d \in \mathbb{Z}$. Esta reducción al caso primo es el principio de muchas demostraciones del teorema de los cuatro cuadrados.

2 El teorema de Minkowski

Primero necesitamos un par de definiciones. Un **retículo** en el espacio vectorial \mathbb{R}^n es un subconjunto

$$\Lambda = \{a_1 \underline{\omega}_1 + \cdots + a_n \underline{\omega}_n \mid a_i \in \mathbb{Z}\}$$

donde $\underline{\omega}_1, \dots, \underline{\omega}_n \in \mathbb{R}^n$ son algunos vectores que forman una base de \mathbb{R}^n . El **paralelepípedo fundamental** asociado a $\underline{\omega}_1, \dots, \underline{\omega}_n$ es el conjunto

$$\Pi := \{\lambda_1 \underline{\omega}_1 + \cdots + \lambda_n \underline{\omega}_n \mid 0 \leq \lambda_i < 1\}.$$

Notemos que todo \mathbb{R}^n es la unión *disjunta* de las traslaciones de Π por los vectores de Λ :

$$\mathbb{R}^n = \bigsqcup_{\underline{u} \in \Lambda} (\Pi + \underline{u}).$$

El volumen del paralelepípedo fundamental es el determinante de la matriz formada por los vectores $\underline{\omega}_1, \dots, \underline{\omega}_n$

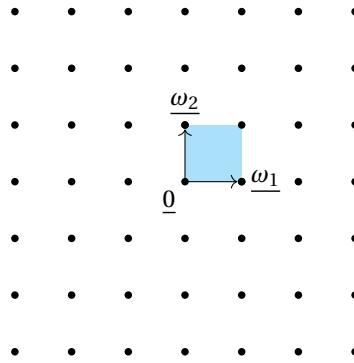
$$\text{vol } \Pi = |\det A|, \quad A = \begin{pmatrix} \underline{\omega}_1 \\ \vdots \\ \underline{\omega}_n \end{pmatrix}$$

(esto es el significado geométrico del determinante).

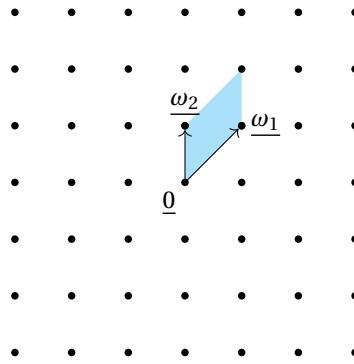
Un típico ejemplo de retículo es

$$\mathbb{Z}^n = \{(a_1, \dots, a_n) \mid a_i \in \mathbb{Z}\} \subset \mathbb{R}^n.$$

Por ejemplo, para $n = 2$ tenemos el siguiente dibujo:



La definición de retículo de arriba no es muy conveniente porque esta depende de una elección de una base particular $\underline{\omega}_1, \dots, \underline{\omega}_n$. El mismo subconjunto $\Lambda \subset \mathbb{R}^n$ puede ser generado por diferentes vectores. Por ejemplo, en el caso de arriba podríamos tomar como otra base



Sin embargo, si $(\underline{\omega}_1, \dots, \underline{\omega}_n)$ y $(\underline{\omega}'_1, \dots, \underline{\omega}'_n)$ son dos bases \mathbb{Z} -lineales de Λ , entonces el cambio de base necesariamente se realiza por una matriz invertible T con elementos enteros:

$$T \in M_n(\mathbb{Z})^\times =: \text{GL}_n(\mathbb{Z}) \iff \det T \in \mathbb{Z}^\times = \{\pm 1\}.$$

Entonces,

$$\det \begin{pmatrix} \underline{\omega}_1 \\ \vdots \\ \underline{\omega}_n \end{pmatrix} = \pm \det \begin{pmatrix} \underline{\omega}'_1 \\ \vdots \\ \underline{\omega}'_n \end{pmatrix}.$$

Esto demuestra que los paralelepípedos fundamentales que corresponden a diferentes bases tienen el mismo volumen. Este es un invariante del conjunto Λ y podemos denotarlo por $\det \Lambda$.

Recordemos que se dice que un subconjunto $X \subseteq \mathbb{R}^n$ es **convexo** si para todo $\underline{x}, \underline{y} \in X$ el segmento de la recta entre \underline{x} e \underline{y} también pertenece a X :

$$(1 - \lambda) \underline{x} + \lambda \underline{y} \in X \quad \text{para todo } \lambda \in [0, 1].$$

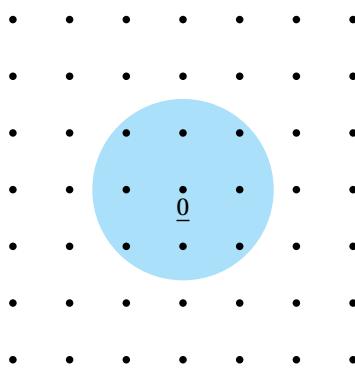
Además, se dice que X es **simétrico** (respecto al origen), si para todo $\underline{x} \in X$ también $-\underline{x} \in X$.

El teorema de Minkowski nos dice algo intuitivamente claro: si X es un conjunto convexo simétrico suficientemente grande, entonces X debe contener puntos no nulos del retículo.

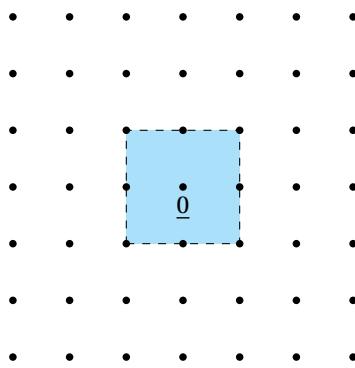
Teorema (Minkowski). *Sea $\Lambda \subset \mathbb{R}^n$ un retículo y sea $X \subseteq \mathbb{R}^n$ un conjunto convexo simétrico tal que*

$$\text{vol } X > 2^n \det \Lambda.$$

Entonces, X contiene un punto no nulo de Λ .



Para entender el significado del múltiplo 2^n en la cota del teorema, podemos considerar el hipercubo abierto con 2^n vértices en $(\pm 1, \pm 1, \dots, \pm 1)$. Consideraremos el retículo $\Lambda := \mathbb{Z}^n \subset \mathbb{R}^n$. El volumen del cubo es $2^n = \det \Lambda$, pero el cubo no contiene ningún punto de Λ salvo $\underline{0}$.



Para demostrar el teorema, necesitamos el siguiente resultado auxiliar.

Lema (Blichfeldt). *Sea $X \subset \mathbb{R}^n$ un conjunto medible*. Si $\text{vol } X > \det \Lambda$, entonces existe un par de puntos diferentes $\underline{x}, \underline{x}' \in X$ tales que $\underline{x} - \underline{x}' \in \Lambda$.*

*En particular, todo conjunto convexo es medible.

Demostración. Puesto que

$$\mathbb{R}^n = \bigsqcup_{\underline{u} \in \Lambda} (\Pi + \underline{u}),$$

tenemos

$$X = \bigsqcup_{\underline{u} \in \Lambda} X \cap (\Pi + \underline{u}),$$

Así que

$$\text{vol } X = \sum_{\underline{u} \in \Lambda} \text{vol}(X \cap (\Pi + \underline{u})) = \sum_{\underline{u} \in \Lambda} \text{vol}((X - \underline{u}) \cap \Pi).$$

Por nuestra hipótesis, $\text{vol } X > \text{vol } \Pi$, de donde los conjuntos

$$(X - \underline{u}) \cap \Pi \subseteq \Pi \quad (\underline{u} \in \Lambda)$$

no pueden ser disjuntos, luego existen $\underline{u}, \underline{u}' \in \Lambda$ tales que

$$(X - \underline{u}) \cap (X - \underline{u}') \neq \emptyset.$$

Tomando

$$\underline{v} \in (X - \underline{u}) \cap (X - \underline{u}'),$$

tenemos

$$\underline{x} = \underline{v} + \underline{u}, \quad \underline{x}' = \underline{v} + \underline{u}' \in X, \quad \underline{x} - \underline{x}' = \underline{u} - \underline{u}' \in \Lambda. \quad \blacksquare$$

Ahora estamos listos para demostrar el teorema de Minkowski. Consideremos el conjunto

$$\frac{1}{2} X := \left\{ \frac{1}{2} \underline{x} \mid \underline{x} \in X \right\}.$$

Tenemos

$$\text{vol} \left(\frac{1}{2} X \right) = \frac{1}{2^n} \text{vol } X > \det \Lambda,$$

así que por el lema de Blichfeldt existen dos puntos distintos $\underline{x}, \underline{x}' \in \frac{1}{2} X$ tales que $\underline{x} - \underline{x}' \in \Lambda$. Para terminar la demostración, sería suficiente ver que este punto pertenece a X . Por la hipótesis que X es simétrico, $-\underline{x}' \in \frac{1}{2} X$ y luego

$$\underline{x} = \frac{1}{2} \underline{y}, \quad -\underline{x}' = \frac{1}{2} \underline{y}' \quad \text{para algunos } \underline{y}, \underline{y}' \in X.$$

El punto

$$\underline{x} - \underline{x}' = \frac{1}{2} \underline{y} + \frac{1}{2} \underline{y}',$$

pertenece a X , siendo una combinación convexa de dos puntos $\underline{y}, \underline{y}' \in X$. ■

3 Ejemplo: el teorema de Fermat sobre dos cuadrados

Para entender mejor el uso del teorema de Minkowski, empecemos por un resultado más sencillo, descubierto en 1640 por Fermat.

Un primo impar p es una suma de dos cuadrados si y solamente si $p \equiv 1 \pmod{4}$.

Por ejemplo,

$$5 = 1^2 + 2^2, \quad 13 = 2^2 + 3^2, \quad 17 = 1^2 + 4^2, \quad 29 = 2^2 + 5^2, \quad 37 = 1^2 + 6^2.$$

(De hecho, la representación $p = a^2 + b^2$ es única salvo una permutación de a y b y sus signos, pero nos contentaremos con una demostración de existencia de estas representaciones.)

3.1. Observación. La condición $p \equiv 1 \pmod{4}$ es necesaria para que p sea una suma de dos cuadrados.

Demostración. Los cuadrados módulo 4 son $0 = 0^2 \equiv 2^2$ y $1 = 1^2 \equiv 3^2$. Luego, a^2 y b^2 no pueden dar el mismo resto módulo 4: en este caso su suma sería par. ■

Recordemos el siguiente resultado.

3.2. Lema. -1 es un residuo cuadrático módulo p si y solamente si $p \not\equiv 3 \pmod{4}$.

Demostración. Necesitamos ver que en el cuerpo finito \mathbb{F}_p se cumple $-1 = x^2$ para algún $x \in \mathbb{F}_p$ si y solamente si $p \not\equiv 3 \pmod{4}$.

Si $p = 2$, entonces $-1 = 1 = 1^2$. Podemos suponer que $p > 2$.

Para $p > 2$ la identidad $-1 = x^2$ en \mathbb{F}_p implica que x es una raíz cuarta primitiva de la unidad:

$$x \neq 1, \quad x^2 = -1 \neq 1, \quad x^3 = -x \neq 1, \quad x^4 = 1.$$

Viceversa, supongamos que existe $x \in \mathbb{F}_p$ tal que

$$x \neq 1, \quad x^2 \neq 1, \quad x^3 \neq 1, \quad x^4 = 1.$$

En particular, $x^2 \neq 1$ implica que también $x \neq -1$. Luego, de la ecuación

$$0 = x^4 - 1 = (x - 1)(x + 1)(x^2 + 1),$$

podemos deducir que $x^2 = -1$.

Esto demuestra que -1 es un residuo cuadrático en \mathbb{F}_p si y solamente si \mathbb{F}_p contiene una raíz cuarta primitiva de la unidad. Esto se reduce a la existencia de un elemento de orden 4 en el grupo \mathbb{F}_p^\times . El último es cíclico de orden $p - 1$ y por lo tanto contiene un elemento de orden 4 si y solamente si

$$4 \mid (p - 1) \iff p - 1 = 4k \text{ para algún } k \iff p \equiv 1 \pmod{4}. \blacksquare$$

Ahora si $p \equiv 1 \pmod{4}$, por el lema de arriba existe $m \in \mathbb{Z}$ tal que

$$1 + m^2 \equiv 0 \pmod{p}.$$

Consideremos los vectores

$$\underline{\omega}_1 := (1, m), \quad \underline{\omega}_2 := (0, p).$$

Estos definen un retículo

$$\Lambda := \{a_1 \underline{\omega}_1 + a_2 \underline{\omega}_2 \mid a_1, a_2 \in \mathbb{Z}\} = \{(a_1, a_1m + a_2p) \mid a_1, a_2 \in \mathbb{Z}\} \subset \mathbb{R}^2.$$

Tenemos

$$\det \Lambda = \det \begin{pmatrix} 1 & m \\ 0 & p \end{pmatrix} = p.$$

3.3. Observación. Para todo $\underline{u} \in \Lambda$ el número $\|\underline{u}\|^2$ es entero y es divisible por p .

Demostración. Si

$$\underline{u} = a_1 \underline{\omega}_1 + a_2 \underline{\omega}_2 = (a_1, a_1m + a_2p),$$

entonces

$$\|\underline{u}\|^2 = a_1^2 + (a_1m + a_2p)^2 = a_1^2(1 + m^2) + 2a_1a_2mp + a_2^2p^2 \equiv a_1^2(1 + m^2) \equiv 0 \pmod{p}. \blacksquare$$

Ahora sea $X \subset \mathbb{R}^2$ el disco abierto de radio $r = \sqrt{2p}$ centrado en el origen:

$$X := \{\underline{x} \in \mathbb{R}^2 \mid \|\underline{x}\|^2 < 2p\}.$$

Es un conjunto convexo simétrico de área

$$\pi r^2 = 2\pi p > 2^2 \det \Lambda = 4p.$$

Entonces, por el teorema de Minkowski, existe un punto $\underline{u} \in \Lambda \setminus \{0\}$ tal que $\underline{u} \in X$. Luego,

$$0 < \|\underline{u}\|^2 < 2p, \quad p \mid \|\underline{u}\|^2.$$

Esto implica que

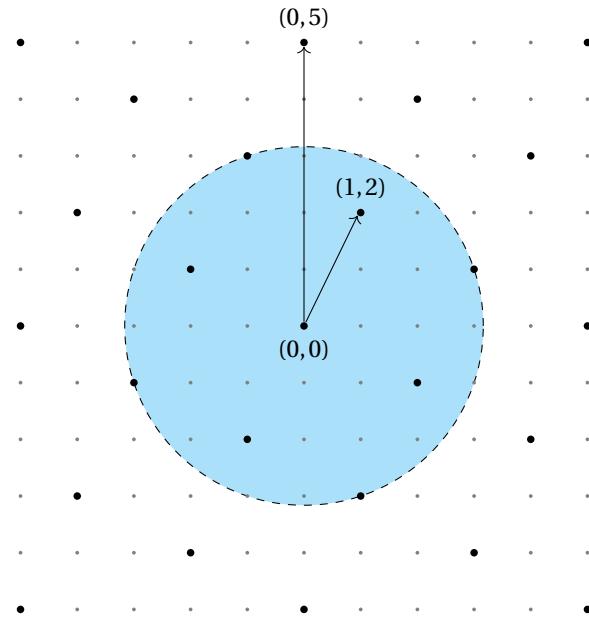
$$p = \|\underline{u}\|^2 = a_1^2 + (a_1 m + a_2 p)^2.$$

Es una representación de p como una suma de dos cuadrados. Esto termina nuestra demostración del resultado de Fermat. ■

Para ver algún ejemplo específico, sea $p = 5$. Tenemos $2^2 + 1 \equiv 0 \pmod{5}$, así que podemos tomar $m = 2$. Luego,

$$\Lambda = \{a_1(1, 2) + a_2(0, 5) \mid a_1, a_2 \in \mathbb{Z}\} = \{(a_1, a_1 \cdot 2 + a_2 \cdot 5) \mid a_1, a_2 \in \mathbb{Z}\} = \{(a_1, a_1 \cdot 2 + a_2 \cdot 5) \mid a_1, a_2 \in \mathbb{Z}\}.$$

Consideremos el siguiente dibujo con Λ y el disco de radio $\sqrt{2p} = \sqrt{10} = 3,16\dots$



Tenemos cuatro puntos no nulos del retículo Λ en el disco: $(\pm 1, \pm 2)$. Estos nos dan

$$5 = 1^2 + 2^2.$$

4 Demostración del teorema de los cuatro cuadrados

Gracias a la identidad de Euler, sería suficiente representar cualquier número primo p como una suma de cuadrados

$$p = a^2 + b^2 + c^2 + d^2.$$

De nuevo, vamos a construir un retículo Λ y un conjunto convexo simétrico X tal que la existencia de un punto no nulo $\underline{x} \in \Lambda$ en X nos da una suma de cuadrados como arriba.

4.1. Lema. Para todo primo p existen $m, n \in \mathbb{Z}$ tales que

$$m^2 + n^2 + 1 \equiv 0 \pmod{p}.$$

Demostración. Si $p = 2$, podemos tomar $m = 1, n = 0$.

Ahora supongamos que $p > 2$. El grupo \mathbb{F}_p^\times es cíclico de orden $p - 1$ y por lo tanto precisamente la mitad de los elementos de \mathbb{F}_p^\times son cuadrados (son las potencias pares de un generador de \mathbb{F}_p^\times):

$$\#\{x^2 \mid x \in \mathbb{F}_p^\times\} = \frac{p-1}{2}.$$

Luego,

$$\#\{x^2 \mid x \in \mathbb{F}_p\} = \frac{p-1}{2} + 1 = \frac{p+1}{2}.$$

Además, tenemos

$$\#\{-1 - y^2 \mid y \in \mathbb{F}_p\} = \frac{p+1}{2}.$$

Se sigue que

$$\{x^2 \mid x \in \mathbb{F}_p\} \cap \{-1 - y^2 \mid y \in \mathbb{F}_p\} \neq \emptyset;$$

es decir,

$$x^2 + y^2 + 1 = 0$$

para algunos $x, y \in \mathbb{F}_p$. ■

Fijemos dos números enteros m y n tales que

$$m^2 + n^2 + 1 \equiv 0 \pmod{p}.$$

Consideremos los siguientes vectores en \mathbb{R}^4 :

$$\underline{\omega}_1 = (1, 0, m, n), \quad \underline{\omega}_2 = (0, 1, n, -m), \quad \underline{\omega}_3 = (0, 0, p, 0), \quad \underline{\omega}_4 = (0, 0, 0, p).$$

Son linealmente independientes. De hecho, podemos calcular el determinante de la matriz formada por ellos:

$$\det \begin{pmatrix} 1 & 0 & m & n \\ 0 & 1 & n & -m \\ 0 & 0 & p & 0 \\ 0 & 0 & 0 & p \end{pmatrix} = p^2$$

(es una matriz triangular). Esto quiere decir que

$$\Lambda := \{a_1 \underline{\omega}_1 + a_2 \underline{\omega}_2 + a_3 \underline{\omega}_3 + a_4 \underline{\omega}_4 \mid a_1, a_2, a_3, a_4 \in \mathbb{Z}\} \subset \mathbb{R}^4$$

es un retículo y

$$\det \Lambda = p^2.$$

4.2. Observación. Para todo $\underline{u} \in \Lambda$ el número $\|\underline{u}\|^2$ es entero y es divisible por p .

Demostración. Si

$$\underline{u} = a_1 \underline{\omega}_1 + a_2 \underline{\omega}_2 + a_3 \underline{\omega}_3 + a_4 \underline{\omega}_4 = (a_1, a_2, a_1 m + a_2 n + a_3 p, a_1 n - a_2 m + a_4 p),$$

entonces

$$\begin{aligned} \|\underline{u}\|^2 &= a_1^2 + a_2^2 + (a_1 m + a_2 n + a_3 p)^2 + (a_1 n - a_2 m + a_4 p)^2 \\ &\equiv a_1^2 + a_2^2 + (a_1 m + a_2 n)^2 + (a_1 n - a_2 m)^2 \pmod{p}. \end{aligned}$$

Luego,

$$a_1^2 + a_2^2 + (a_1 m + a_2 n)^2 + (a_1 n - a_2 m)^2 = (a_1^2 + a_2^2)(m^2 + n^2 + 1)$$

y $m^2 + n^2 + 1 \equiv 0 \pmod{p}$ por nuestra elección de m y n . ■

Sea X la bola abierta en \mathbb{R}^4 de radio $r = \sqrt{2p}$ centrada en el origen:

$$X := \{\underline{x} \in \mathbb{R}^4 \mid \|\underline{x}\|^2 < 2p\}.$$

Recordemos que en general la bola n -dimensional de radio r tiene volumen

$$\frac{\pi^{n/2}}{\Gamma\left(\frac{n}{2} + 1\right)} r^n.$$

En este caso $n = 4$ y $\Gamma\left(\frac{n}{2} + 1\right) = \Gamma(3) = 2! = 2$. Tenemos

$$\text{vol } X = \frac{\pi^2 r^4}{2} = 2\pi^2 p^2 > 2^4 \det \Lambda = 16 p^2$$

(de hecho, $2\pi^2 = 19,73\dots > 16$). Entonces, según el teorema de Minkowski, existe un punto $\underline{u} \in \Lambda \setminus \{0\}$ tal que $\underline{u} \in X$. De las desigualdades

$$0 < \|\underline{u}\|^2 < 2p, \quad p \mid \|\underline{u}\|^2.$$

podemos concluir que

$$\|\underline{u}\|^2 = p.$$

Esto nos da una representación de p como una suma de cuatro cuadrados. ■

Apéndice. Algunas sumas de cuatro cuadrados

$$1 = 1^2$$

$$2 = 1^2 + 1^2$$

$$3 = 1^2 + 1^2 + 1^2$$

$$\begin{aligned} 4 &= 1^2 + 1^2 + 1^2 + 1^2 \\ &= 2^2 \end{aligned}$$

$$5 = 2^2 + 1^2$$

$$6 = 2^2 + 1^2 + 1^2$$

$$7 = 2^2 + 1^2 + 1^2 + 1^2$$

$$8 = 2^2 + 2^2$$

$$\begin{aligned} 9 &= 2^2 + 2^2 + 1^2 \\ &= 3^2 \end{aligned}$$

$$\begin{aligned} 10 &= 2^2 + 2^2 + 1^2 + 1^2 \\ &= 3^2 + 1^2 \end{aligned}$$

$$11 = 3^2 + 1^2 + 1^2$$

$$\begin{aligned} 12 &= 2^2 + 2^2 + 2^2 \\ &= 3^2 + 1^2 + 1^2 + 1^2 \end{aligned}$$

$$\begin{aligned} 13 &= 2^2 + 2^2 + 2^2 + 1^2 \\ &= 3^2 + 2^2 \end{aligned}$$

$$14 = 3^2 + 2^2 + 1^2$$

$$15 = 3^2 + 2^2 + 1^2 + 1^2$$

$$\begin{aligned} 16 &= 2^2 + 2^2 + 2^2 + 2^2 \\ &= 4^2 \end{aligned}$$

$$\begin{aligned} 17 &= 3^2 + 2^2 + 2^2 \\ &= 4^2 + 1^2 \end{aligned}$$

$$\begin{aligned} 18 &= 3^2 + 2^2 + 2^2 + 1^2 \\ &= 3^2 + 3^2 \\ &= 4^2 + 1^2 + 1^2 \end{aligned}$$

$$\begin{aligned} 19 &= 3^2 + 3^2 + 1^2 \\ &= 4^2 + 1^2 + 1^2 + 1^2 \end{aligned}$$

$$\begin{aligned} 20 &= 3^2 + 3^2 + 1^2 + 1^2 \\ &= 4^2 + 2^2 \end{aligned}$$

$$\begin{aligned} 21 &= 3^2 + 2^2 + 2^2 + 2^2 \\ &= 4^2 + 2^2 + 1^2 \end{aligned}$$

$$\begin{aligned} 22 &= 3^2 + 3^2 + 2^2 \\ &= 4^2 + 2^2 + 1^2 + 1^2 \end{aligned}$$

$$23 = 3^2 + 3^2 + 2^2 + 1^2$$

$$24 = 4^2 + 2^2 + 2^2$$

$$\begin{aligned} 25 &= 4^2 + 2^2 + 2^2 + 1^2 \\ &= 4^2 + 3^2 \end{aligned}$$

$$\begin{aligned} 26 &= 3^2 + 3^2 + 2^2 + 2^2 \\ &= 4^2 + 3^2 + 1^2 \end{aligned}$$

$$= 5^2 + 1^2$$

$$\begin{aligned} 27 &= 3^2 + 3^2 + 3^2 \\ &= 4^2 + 3^2 + 1^2 + 1^2 \\ &= 5^2 + 1^2 + 1^2 \end{aligned}$$

$$\begin{aligned} 28 &= 3^2 + 3^2 + 3^2 + 1^2 \\ &= 4^2 + 2^2 + 2^2 + 2^2 \\ &= 5^2 + 1^2 + 1^2 + 1^2 \end{aligned}$$

$$\begin{aligned} 29 &= 4^2 + 3^2 + 2^2 \\ &= 5^2 + 2^2 \end{aligned}$$

$$\begin{aligned} 30 &= 4^2 + 3^2 + 2^2 + 1^2 \\ &= 5^2 + 2^2 + 1^2 \end{aligned}$$

$$\begin{aligned} 31 &= 3^2 + 3^2 + 3^2 + 2^2 \\ &= 5^2 + 2^2 + 1^2 + 1^2 \end{aligned}$$

$$32 = 4^2 + 4^2$$

$$\begin{aligned} 33 &= 4^2 + 3^2 + 2^2 + 2^2 \\ &= 4^2 + 4^2 + 1^2 \\ &= 5^2 + 2^2 + 2^2 \end{aligned}$$

$$\begin{aligned} 34 &= 4^2 + 3^2 + 3^2 \\ &= 4^2 + 4^2 + 1^2 + 1^2 \\ &= 5^2 + 2^2 + 2^2 + 1^2 \\ &= 5^2 + 3^2 \end{aligned}$$

$$\begin{aligned} 35 &= 4^2 + 3^2 + 3^2 + 1^2 \\ &= 5^2 + 3^2 + 1^2 \end{aligned}$$

$$\begin{aligned} 36 &= 3^2 + 3^2 + 3^2 + 3^2 \\ &= 4^2 + 4^2 + 2^2 \\ &= 5^2 + 3^2 + 1^2 + 1^2 \\ &= 6^2 \end{aligned}$$

$37 = 4^2 + 4^2 + 2^2 + 1^2$	$46 = 5^2 + 4^2 + 2^2 + 1^2$	$54 = 5^2 + 4^2 + 3^2 + 2^2$
$= 5^2 + 2^2 + 2^2 + 2^2$	$= 6^2 + 3^2 + 1^2$	$= 5^2 + 5^2 + 2^2$
$= 6^2 + 1^2$		$= 6^2 + 3^2 + 3^2$
$38 = 4^2 + 3^2 + 3^2 + 2^2$	$47 = 5^2 + 3^2 + 3^2 + 2^2$	$= 6^2 + 4^2 + 1^2 + 1^2$
$= 5^2 + 3^2 + 2^2$	$= 6^2 + 3^2 + 1^2 + 1^2$	$= 7^2 + 2^2 + 1^2$
$= 6^2 + 1^2 + 1^2$		
$39 = 5^2 + 3^2 + 2^2 + 1^2$	$48 = 4^2 + 4^2 + 4^2$	$55 = 5^2 + 5^2 + 2^2 + 1^2$
$= 6^2 + 1^2 + 1^2 + 1^2$	$= 6^2 + 2^2 + 2^2 + 2^2$	$= 6^2 + 3^2 + 3^2 + 1^2$
$40 = 4^2 + 4^2 + 2^2 + 2^2$	$49 = 4^2 + 4^2 + 4^2 + 1^2$	$= 7^2 + 2^2 + 1^2 + 1^2$
$= 6^2 + 2^2$	$= 5^2 + 4^2 + 2^2 + 2^2$	
	$= 6^2 + 3^2 + 2^2$	
	$= 7^2$	
$41 = 4^2 + 4^2 + 3^2$	$50 = 4^2 + 4^2 + 3^2 + 3^2$	$56 = 6^2 + 4^2 + 2^2$
$= 5^2 + 4^2$	$= 5^2 + 4^2 + 3^2$	
$= 6^2 + 2^2 + 1^2$	$= 5^2 + 5^2$	
	$= 6^2 + 3^2 + 2^2 + 1^2$	
$42 = 4^2 + 4^2 + 3^2 + 1^2$	$= 7^2 + 1^2$	
$= 5^2 + 3^2 + 2^2 + 2^2$		
$= 5^2 + 4^2 + 1^2$	$51 = 5^2 + 4^2 + 3^2 + 1^2$	
$= 6^2 + 2^2 + 1^2 + 1^2$	$= 5^2 + 5^2 + 1^2$	
	$= 7^2 + 1^2 + 1^2$	
$43 = 4^2 + 3^2 + 3^2 + 3^2$		$58 = 5^2 + 4^2 + 4^2 + 1^2$
$= 5^2 + 3^2 + 3^2$	$52 = 4^2 + 4^2 + 4^2 + 2^2$	$= 5^2 + 5^2 + 2^2 + 2^2$
$= 5^2 + 4^2 + 1^2 + 1^2$	$= 5^2 + 3^2 + 3^2 + 3^2$	$= 6^2 + 3^2 + 3^2 + 2^2$
	$= 5^2 + 5^2 + 1^2 + 1^2$	$= 7^2 + 2^2 + 2^2 + 1^2$
$44 = 5^2 + 3^2 + 3^2 + 1^2$	$= 6^2 + 4^2$	$= 7^2 + 3^2$
$= 6^2 + 2^2 + 2^2$	$= 7^2 + 1^2 + 1^2 + 1^2$	
$45 = 4^2 + 4^2 + 3^2 + 2^2$	$53 = 6^2 + 3^2 + 2^2 + 2^2$	$59 = 5^2 + 4^2 + 3^2 + 3^2$
$= 5^2 + 4^2 + 2^2$	$= 6^2 + 4^2 + 1^2$	$= 5^2 + 5^2 + 3^2$
$= 6^2 + 2^2 + 2^2 + 1^2$	$= 7^2 + 2^2$	$= 7^2 + 3^2 + 1^2$
$= 6^2 + 3^2$		

$62 = 6^2 + 4^2 + 3^2 + 1^2$	$69 = 6^2 + 4^2 + 4^2 + 1^2$	$76 = 5^2 + 5^2 + 5^2 + 1^2$
$= 6^2 + 5^2 + 1^2$	$= 6^2 + 5^2 + 2^2 + 2^2$	$= 6^2 + 6^2 + 2^2$
$= 7^2 + 3^2 + 2^2$	$= 7^2 + 4^2 + 2^2$	$= 7^2 + 3^2 + 3^2 + 3^2$
	$= 8^2 + 2^2 + 1^2$	$= 7^2 + 5^2 + 1^2 + 1^2$
$63 = 5^2 + 5^2 + 3^2 + 2^2$	$70 = 5^2 + 5^2 + 4^2 + 2^2$	$= 8^2 + 2^2 + 2^2 + 2^2$
$= 6^2 + 3^2 + 3^2 + 3^2$	$= 6^2 + 4^2 + 3^2 + 3^2$	$77 = 6^2 + 4^2 + 4^2 + 3^2$
$= 6^2 + 5^2 + 1^2 + 1^2$	$= 6^2 + 5^2 + 3^2$	$= 6^2 + 5^2 + 4^2$
$= 7^2 + 3^2 + 2^2 + 1^2$	$= 7^2 + 4^2 + 2^2 + 1^2$	$= 6^2 + 6^2 + 2^2 + 1^2$
$64 = 4^2 + 4^2 + 4^2 + 4^2$	$= 8^2 + 2^2 + 1^2 + 1^2$	$= 8^2 + 3^2 + 2^2$
$= 8^2$		
$65 = 6^2 + 4^2 + 3^2 + 2^2$	$71 = 6^2 + 5^2 + 3^2 + 1^2$	$78 = 6^2 + 5^2 + 4^2 + 1^2$
$= 6^2 + 5^2 + 2^2$	$= 7^2 + 3^2 + 3^2 + 2^2$	$= 7^2 + 4^2 + 3^2 + 2^2$
$= 7^2 + 4^2$		$= 7^2 + 5^2 + 2^2$
$= 8^2 + 1^2$	$72 = 6^2 + 4^2 + 4^2 + 2^2$	$= 8^2 + 3^2 + 2^2 + 1^2$
	$= 6^2 + 6^2$	
	$= 8^2 + 2^2 + 2^2$	
$66 = 5^2 + 4^2 + 4^2 + 3^2$	$73 = 5^2 + 4^2 + 4^2 + 4^2$	$79 = 5^2 + 5^2 + 5^2 + 2^2$
$= 5^2 + 5^2 + 4^2$	$= 6^2 + 6^2 + 1^2$	$= 6^2 + 5^2 + 3^2 + 3^2$
$= 6^2 + 5^2 + 2^2 + 1^2$	$= 7^2 + 4^2 + 2^2 + 2^2$	$= 7^2 + 5^2 + 2^2 + 1^2$
$= 7^2 + 3^2 + 2^2 + 2^2$	$= 8^2 + 2^2 + 2^2 + 1^2$	$80 = 6^2 + 6^2 + 2^2 + 2^2$
$= 7^2 + 4^2 + 1^2$	$= 8^2 + 3^2$	$= 8^2 + 4^2$
$= 8^2 + 1^2 + 1^2$		
$67 = 5^2 + 5^2 + 4^2 + 1^2$	$74 = 6^2 + 5^2 + 3^2 + 2^2$	$81 = 6^2 + 5^2 + 4^2 + 2^2$
$= 7^2 + 3^2 + 3^2$	$= 6^2 + 6^2 + 1^2 + 1^2$	$= 6^2 + 6^2 + 3^2$
$= 7^2 + 4^2 + 1^2 + 1^2$	$= 7^2 + 4^2 + 3^2$	$= 7^2 + 4^2 + 4^2$
$= 8^2 + 1^2 + 1^2 + 1^2$	$= 7^2 + 5^2$	$= 8^2 + 3^2 + 2^2 + 2^2$
	$= 8^2 + 3^2 + 1^2$	$= 8^2 + 4^2 + 1^2$
$68 = 5^2 + 5^2 + 3^2 + 3^2$	$75 = 5^2 + 5^2 + 4^2 + 3^2$	$= 9^2$
$= 6^2 + 4^2 + 4^2$	$= 5^2 + 5^2 + 5^2$	$82 = 5^2 + 5^2 + 4^2 + 4^2$
$= 7^2 + 3^2 + 3^2 + 1^2$	$= 7^2 + 4^2 + 3^2 + 1^2$	$= 6^2 + 6^2 + 3^2 + 1^2$
$= 8^2 + 2^2$	$= 7^2 + 5^2 + 1^2$	$= 7^2 + 4^2 + 4^2 + 1^2$
	$= 8^2 + 3^2 + 1^2 + 1^2$	$= 7^2 + 5^2 + 2^2 + 2^2$
		$= 8^2 + 3^2 + 3^2$
		$= 8^2 + 4^2 + 1^2 + 1^2$
		$= 9^2 + 1^2$

$83 = 7^2 + 4^2 + 3^2 + 3^2$	$90 = 6^2 + 5^2 + 5^2 + 2^2$	$96 = 8^2 + 4^2 + 4^2$
$= 7^2 + 5^2 + 3^2$	$= 6^2 + 6^2 + 3^2 + 3^2$	$97 = 6^2 + 6^2 + 4^2 + 3^2$
$= 8^2 + 3^2 + 3^2 + 1^2$	$= 7^2 + 4^2 + 4^2 + 3^2$	$= 6^2 + 6^2 + 5^2$
$= 9^2 + 1^2 + 1^2$	$= 7^2 + 5^2 + 4^2$	$= 7^2 + 4^2 + 4^2 + 4^2$
 	$= 7^2 + 6^2 + 2^2 + 1^2$	$= 8^2 + 4^2 + 4^2 + 1^2$
$84 = 5^2 + 5^2 + 5^2 + 3^2$	$= 8^2 + 4^2 + 3^2 + 1^2$	$= 8^2 + 5^2 + 2^2 + 2^2$
$= 6^2 + 4^2 + 4^2 + 4^2$	$= 8^2 + 5^2 + 1^2$	$= 9^2 + 4^2$
$= 7^2 + 5^2 + 3^2 + 1^2$	$= 9^2 + 2^2 + 2^2 + 1^2$	
$= 8^2 + 4^2 + 2^2$	$= 9^2 + 3^2$	
$= 9^2 + 1^2 + 1^2 + 1^2$		
$85 = 6^2 + 6^2 + 3^2 + 2^2$	$91 = 5^2 + 5^2 + 5^2 + 4^2$	$98 = 6^2 + 6^2 + 5^2 + 1^2$
$= 7^2 + 4^2 + 4^2 + 2^2$	$= 7^2 + 5^2 + 4^2 + 1^2$	$= 7^2 + 6^2 + 3^2 + 2^2$
$= 7^2 + 6^2$	$= 8^2 + 3^2 + 3^2 + 3^2$	$= 7^2 + 7^2$
$= 8^2 + 4^2 + 2^2 + 1^2$	$= 8^2 + 5^2 + 1^2 + 1^2$	$= 8^2 + 4^2 + 3^2 + 3^2$
$= 9^2 + 2^2$	$= 9^2 + 3^2 + 1^2$	$= 8^2 + 5^2 + 3^2$
 		$= 9^2 + 3^2 + 2^2 + 2^2$
$86 = 6^2 + 5^2 + 4^2 + 3^2$	$92 = 6^2 + 6^2 + 4^2 + 2^2$	$= 9^2 + 4^2 + 1^2$
$= 6^2 + 5^2 + 5^2$	$= 7^2 + 5^2 + 3^2 + 3^2$	$99 = 7^2 + 5^2 + 4^2 + 3^2$
$= 7^2 + 6^2 + 1^2$	$= 9^2 + 3^2 + 1^2 + 1^2$	$= 7^2 + 5^2 + 5^2$
$= 8^2 + 3^2 + 3^2 + 2^2$		$= 7^2 + 7^2 + 1^2$
$= 9^2 + 2^2 + 1^2$	 	$= 8^2 + 5^2 + 3^2 + 1^2$
 	$93 = 6^2 + 5^2 + 4^2 + 4^2$	$= 9^2 + 3^2 + 3^2$
$87 = 6^2 + 5^2 + 5^2 + 1^2$	$= 7^2 + 6^2 + 2^2 + 2^2$	$= 9^2 + 4^2 + 1^2 + 1^2$
$= 7^2 + 5^2 + 3^2 + 2^2$	$= 8^2 + 4^2 + 3^2 + 2^2$	
$= 7^2 + 6^2 + 1^2 + 1^2$	$= 8^2 + 5^2 + 2^2$	
$= 9^2 + 2^2 + 1^2 + 1^2$	$= 9^2 + 2^2 + 2^2 + 2^2$	
 		$100 = 5^2 + 5^2 + 5^2 + 5^2$
$88 = 6^2 + 6^2 + 4^2$	$94 = 7^2 + 5^2 + 4^2 + 2^2$	$= 7^2 + 5^2 + 5^2 + 1^2$
$= 8^2 + 4^2 + 2^2 + 2^2$	$= 7^2 + 6^2 + 3^2$	$= 7^2 + 7^2 + 1^2 + 1^2$
 	$= 8^2 + 5^2 + 2^2 + 1^2$	$= 8^2 + 4^2 + 4^2 + 2^2$
$89 = 6^2 + 6^2 + 4^2 + 1^2$	$= 9^2 + 3^2 + 2^2$	$= 8^2 + 6^2$
$= 7^2 + 6^2 + 2^2$		$= 9^2 + 3^2 + 3^2 + 1^2$
$= 8^2 + 4^2 + 3^2$	 	$= 10^2$
$= 8^2 + 5^2$		
$= 9^2 + 2^2 + 2^2$		