Capítulo 4

Ejemplos de ecuaciones diofánticas

En este capítulo estudiaremos ecuaciones donde las variables son números enteros. Se las denomina ecuaciones diofánticas. En capítulos anteriores hemos estudiado ecuaciones lineales de la forma $ax+by=c$. Veíamos que la ecuación tenía soluciones si y sólo si $(a,b)|c$. En ese caso, dividiendo entre (a,b), la ecuación era equivalente a una ecuación de la forma $ax+by=c$ con $(a,b)=1$. Con el algoritmo de Euclides calculábamos una solución (x_1,y_1) de la ecuación $ax+by=1$ lo que nos permitía hallar una solución $(x_0,y_0)=(cx_1,cy_1)$ de la ecuación $ax+by=c$. Finalmente, las infinitas soluciones enteras de esta ecuación venían dadas por $x=x_0+bt,\ y=y_0-at,\ t\in\mathbb{Z}$.

4.1. El problema del cambio de monedas

Supongamos que tenemos monedas de valores $a_1,\ldots,a_k$. El problema del cambio de monedas consiste en hallar qué cantidades podemos lograr utilizando estas monedas. Es decir, para que valores de c la ecuación $a_1x_1+\cdots+a_kx_k=c$ tiene soluciones en enteros no negatios $x_1,\ldots,x_k$. Al valor más pequeño de c con esta propiedad se le denomina $g(a_1,\ldots,a_k)$. Hallar este valor, denominado número de Frobenius, es un problema muy difícil para el cual no existe una fórmula sencilla salvo en el caso $k=2$.

Teorema 4.1.1 (Sylvester, 1884)**.** *Sean a_1 y a_2 enteros positivos y primos entre sí. En este caso, el número de Frobenius es $g(a_1,a_2)=a_1a_2-a_1-a_2$.*

Demostración. De las infinitas soluciones de la ecuación $c=a_1x_1+a_2x_2$ con x_1,x_2 enteros, hay una y sólo una con $0\leq x_1<a_2$. Una consecuencia de esta unicidad es que si (x_1',x_2') es cualquier otra solución de $a_1x_1+a_2x_2=c,\ 0\leq x_1',x_2'$ entonces necesariamente $x_1'>x_1$ y $x_2'<x_2$. Así que la única manera de que la ecuación

tenga alguna solución en enteros no negativos es que el x_2 correspondiente al x_1 con $0 \leq x_1 < a_2$ sea también no negativo.

Si c es tal que $c = a_1x_1 + a_2x_2$ no tiene soluciones no negativas, en la representación con $0 \leq x_1 < a_2$, deberá ocurrir que $x_2 \leq -1$ y c deberá cumplir

$$c = a_1x_1 + a_2x_2 \leq a_1(a_2 - 1) + a_2(-1) = a_1a_2 - a_1 - a_2.$$

Sólo nos falta ver que $c = a_1a_1 - a_1 - a_2$ no se puede representar con soluciones no negativas. Pero eso es claro porque

$$a_1a_2 - a_1 - a_2 = a_1x_1 + a_2x_2$$

para $x_1 = a_2 - 1$ y $x_2 = -1$ y cualquier otra solución, (x_1', x_2'), bien $x_1' < 0$ o bien $x_2' < x_2 \leq -1$. □

4.2. Algunos casos del ltimo Teorema de Fermat

La ecuación $x^n + y^n = z^n,\ xyz \neq 0$ es sin lugar a dudas la más famosa de todas las ecuaciones diofánticas. Pierre de Fermat (1601-65) dijo haber demostrado que to tenía soluciones enteras para $n \geq 3$, pero que la bella demostración que había obtenido era demasiado larga para poder escribirla en los márgenes de su ejemplar del libro de Diofanto, como acostumbraba a hacer con muchas de sus observaciones. Este problema conocido como el Último Teorema de Fermat fue resuelto por Andrew Wiles en 1995. La demostración de Wiles sobrepasa con creces los propósitos de este libro, y nos conformaremos estudiando la ecuación de Fermat para los casos $n = 2, 3$ y 4.

4.2.1. Las ternas pitagóricas

Las ternas (x, y, z) tales que $x^2 + y^2 = z^2$ se denomina ternas pitagóricas y originan triángulos rectángulos con lados enteros. Estudiaremos ecuaciones más generales del tipo

$$ax^2 + by^2 = cz^2,\ a, b, c \in \mathbb{Z}.$$

En general esta ecuación no tiene por qué tener soluciones, pero si encontramos una solución (x_0, y_0, z_0) vamos a poder hallar el resto por un procedimiento sencillo.

Observemos que buscar las soluciones enteras de $ax^2 + by^2 = cz^2$ es equivalente a buscar las soluciones racionales de $ax_1^2 + by_1^2 = c$, donde hemos hecho $x_1 = x/z,\ y_1 = y/z$. Es decir, habremos de encontrar los puntos (x, y) de coordenadas racionales sobre la elipse $ax^2 + by^2 = c$.

Supongamos que mediante una simple inspección hemos encontrado un punto (x_0, y_0) de coordenadas racionales sobre la elipse. Ahora trazamos una recta que pase por dicho punto y con pendiente $r \in Q$. Esta recta cortará a la elipse en otro punto (x_0', y_0').

Si $y - y_0 = r(x - x_0)$ es la ecuación de la recta y la sustituimos en la ecuación de la elipse, $ax^2 + b(y_0 + r(x - x_0))^2 = c$ obtenemos una ecuación de segundo grado que tendrá como soluciones x_0 y x_0'.

Ahora bien, la suma de las soluciones de una ecuación de segundo grado con coeficientes racionales es racional. Por lo tanto, si x_0 era racional, x_0' debe ser racional y sustituyendo en la recta anterior tenemos que y_0' también es racional.

Por otra parte, dos puntos de coordenadas racionales sobre la elipse nos determinan una recta de pendiente racional. Es decir, existe una biyección entre las soluciones enteras de la ecuación original y los puntos x_0', y_0' obtenidos según el método anterior.

Ahora estamos en condiciones de demostrar nuestro primer teorema.

Teorema 4.2.1. *Todas las soluciones enteras de la ecuación $x^2 + y^2 = z^2$ vienen dadas por la fórmula*

$$\begin{cases} x = (n^2 - m^2)t \\ y = 2mnt \\ z = (n^2 + m^2)t \end{cases}$$

donde $t \in \mathbb{Z}$ y n, m son enteros primos entre sí y de distinta paridad.

Demostración. Empezaremos calculando las soluciones primitivas entre sí, $(x, y) = (x, z) = (y, z) = 1$. Intentaremos hallar todas las soluciones racionales de la ecuación $x^2 + y^2 = 1$ a partir de la solución $(x_0, y_0) = (1, 0)$.

Trazaremos una recta de pendiente $\frac{n}{m}$ (fracción irreducible) que pase por el punto $(1, 0)$. Esta es la recta $y = \frac{n}{m}(x-1)$. Ahora calculamos su punto de intersección con la elipse resolviendo la ecuación

$$x^2 + \left(\frac{n}{m}(x - 1)\right)^2 = 1.$$

Así obtenemos $x_0 = 1$, la solución de la que partíamos, y $x_0' = \frac{n^2-m^2}{n^2+m^2}$.

Sustituyendo en la recta obtenemos $y_0' = -\frac{2mn}{n^2+m^2}$. Es decir,

$$\left(\frac{n^2 - m^2}{n^2 + m^2}\right)^2 + \left(\frac{2mn}{n^2 + m^2}\right)^2 = 1,$$

y por lo tanto

$$(n^2 - m^2)^2 + (2mn)^2 = (n^2 + m^2)^2.$$

Entonces $x = n^2 - m^2,\ y = 2mn,\ z = m^2 + n^2$ y como estamos pidiendo que las soluciones sean primitivas, además de que $(n, m) = 1$ debe ocurrir que n y m deben de tener distinta paridad. El resto de las soluciones vienen de multiplicar x, y, z por un mismo entero t. □

4.2.2. La ecuación $x^4 + y^4 = z^2$

Aunque ya hemos señalado que la demostración del Último Teorema de Fermat es realmente difícil, hay algunos exponentes n para los que la demostración está al nivel de este curso.

Empezaremos haciéndolo para $n = 4$ utilizando para ello el llamado método del descenso, inventado por Fermat y de uso muy frecuente en la teoría de los números. De hecho demostraremos un poco más:

Teorema 4.2.2. *La ecuación $x^4+y^4 = z^2$ no tiene soluciones en enteros si $xyz \neq 0$.*

Demostración. Supongamos que nuestra ecuación tiene alguna solución. De todas las soluciones que pueda tener elijamos la solución mínima. Sea u el menor entero positivo tal que $x^4 + y^4 = u^2$ para algún x, y.

A partir de esta solución encontraremos una solución menor obteniendo así una contradicción (Método del descenso).

La ecuación $x^4 + y^4 = u^2$ se puede expresar como una terna pitagórica $(x^2)^2 + (y^2)^2 = u^2$.

Obviamente $(x, y) = 1$. Si $(x, y) = d$ tendríamos $\left(\frac{x}{d}\right)^4 + \left(\frac{y}{d}\right)^4 = \left(\frac{u}{d^2}\right)^2$ obteninedo una solución menor.

Por el teorema 5.2.1 tenemos

$$\begin{cases} x^2 = n^2 - m^2 \\ y^2 = 2mn \\ n = m^2 + n^2 \end{cases}$$

para algún par m, n con $(m, n) = 1$ y de distinta paridad.

Si n es par entonce $x^2 = n^2 - m^2 \equiv -1$ (mód 4), lo cual es imposible porque -1 no es un residuo cuadrático módulo 4. Entonces n es impar y m es par. Si escribimos $m = 2m'$ tenemos que $(y/2)^2 = nm'$. Es claro que si $(n, m) = 1$ entonces

$(n, m') = 1$. Y como su producto es un cuadrado, entonces cada uno de ellos ha de ser un cuadrado: $n = b^2, \quad m' = a^2$.

Tenemos entonces que $x^2 = n^2 - m^2 = b^4 - 4a^4$. Es decir, $(2a^2)^2 + x^2 = (b^2)^2$ y nos encontramos con otra terna pitagórica. Aplicando de nuevo el teorema 5.2.1,

$$\begin{cases} 2a^2 = 2rs \\ x^2 = r^2 - s^2 \\ b^2 = r^2 + s^2 \end{cases}$$

con $(r, s) = 1$ y de distinta paridad.

De nuevo tenemos dos enteros r, s primos entre sí y cuyo producto es un cuadrado y por lo tanto lo son cada uno de ellos: $r = c^2, \quad s = d^2$.

Sustituyendo obtenemos $c^4 + d^4 = b^2$, una solución de nuestra ecuación original. Pero $b < b^4 + m^2 = u$ contradiciendo el hecho de que u era la mínima solución posible. □

4.2.3. La ecuación $x^3 + y^3 = z^3$

Antes de estudiar esta ecuación haremos algunas observaciones sobre el anillo

$$\mathbb{Z}[\omega] = \{a + b\omega : \quad a, b \in \mathbb{Z}\},$$

donde $\omega = e^{2\pi/3}$, raíz cúbica de la unidad. Las demostraciones se dejan como ejercicio.

1) $1 + \omega + \omega^2 = 0$ y $\overline{\omega} = \omega^2$.

2) $N(a + b\omega) = a^2 - ab + b^2$.

3) Las unidades de $\mathbb{Z}[\omega]$ son $\{\pm 1, \pm\omega, \pm\omega^2\}$.

4) Si $N(a + b\omega)$ es un primo en $\mathbb{Z}$, entonces $a + b\omega$ es un primo en $\mathbb{Z}[\omega]$.

5) El anillo $\mathbb{Z}[\omega]$ es un anillo euclídeo y por tanto de factorización única. Todo entero se descompone en sus factores primos de manera única excepto el orden y las unidades.

6) El entero $1 - \omega$ es primo en $\mathbb{Z}$.

La aritmética de $\mathbb{Z}[\omega]$ tiene gran interés, ya que precisamente es en $\mathbb{Z}[\omega]$ donde la ecuación $x^3 + y^3 = z^3$ se factoriza:

$$x^3 + y^3 = (x + y)(x\omega + y\omega^2)(x\omega^2 + y\omega) = z^3.$$

Teorema 4.2.3. *La ecuación $x^3+y^3=z^3,\ xyz\neq 0$ no tiene soluciones en enteros.*

Demostración. De hecho demostraremos algo más: la ecuación anterior no tiene soluciones en $\mathbb{Z}[\omega]$.

Supongamos que x, y, z son tres elementos no nulos de $\mathbb{Z}[\omega]$ tales que $x^3+y^3=z^3$. No hay nada que nos impida suponer que x, y, z son primos relativos dos a dos en $\mathbb{Z}[\omega]$. Si $d\in\mathbb{Z}[\omega]$ dividiera a dos de ellos, podríamos dividir la ecuación entre d^3 y $x/d, y/d, z/z$ sería una solución de la ecuación.

Lema 4.2.4. $a+b\omega\equiv 0,1\ ó\ -1\ (\text{mód } 1-\omega)$.

Demostración. Observemos que $a+b\omega\equiv a+b\ (\text{mód } 1-\omega)$. Por otra parte $a+b=3q+r,\ 0\leq r<3$. Entonces,

$$a+b\omega\equiv a+b\equiv 3q+r\equiv r\quad(\text{mód } 1-\omega)$$

porque 3 es un múltiplo de $1-\omega$ en $\mathbb{Z}[\omega]$. Concretamente $3=-\omega^2(1-\omega)^2$. □

Lema 4.2.5. *Si $\alpha\in\mathbb{Z}[\omega]$ y $\alpha\equiv\pm 1\ (\text{mód } 1-\omega)$, entonces $\alpha^3\equiv\pm 1\ (\text{mód } (1-\omega)^4)$.*

Demostración. Como $\alpha\equiv\pm 1\ (\text{mód } 1-\omega)$ entonces $\alpha=\beta(1-\omega)\pm 1$ para algún entero $\beta\in\mathbb{Z}[\omega]$.

Elevando al cubo,

$$\alpha^3=\beta^3(1-\omega)^3\pm 3\beta^2(1-\omega)^2+3\beta(1-\omega)\pm 1.$$

Observando que $3=-\omega^2(1-\omega)^2$ y sustituyendo tenemos

$$\begin{aligned}\alpha^3&=\beta^3(1-\omega)^3\pm(-\omega^2)(1-\omega)^4\beta^2-\omega^2\beta(1-\omega)^3\pm 1\\&=(1-\omega)^3\beta(\beta^2-\omega^2)\pm(-\omega^2)\beta^2(1-\omega)^4\pm 1.\end{aligned}$$

Para terminar la demostración debemos ver que $(1-\omega)^3\beta(\beta^2-\omega^2)\equiv 0\ (\text{mód } (1-\omega)^4)$. Es decir, debemos ver que $\beta(\beta^2-\omega^2)\equiv 0\ (\text{mód } 1-\omega)$.

Si $\beta\equiv 0\ (\text{mód } 1-\omega)$, ya está demostrado. En otro caso, por el lema anterior, $\beta\equiv\pm 1\ (\text{mód } 1-\omega)$ y entonces $\beta^2\equiv 1\ (\text{mód } 1-\omega)$. Por tanto $\beta^2-\omega^2\equiv 0\ (\text{mód } 1-\omega)$ y el lema queda demostrado. □

Lema 4.2.6. *Si $x^3+y^3=z^3$ entonces x, y ó z tiene que ser divisible por $1-\omega$.*

Demostración. Por el lema 5.2.5, si ninguno de ellos fuese divisible por $1-\omega$ tendríamos

$$\begin{cases}x^3\equiv\pm 1 & (\text{mód } (1-\omega)^4)\\ y^3\equiv\pm 1 & (\text{mód } (1-\omega)^4)\\ z^3\equiv\pm 1 & (\text{mód } (1-\omega)^4).\end{cases}$$

Entonces $(\pm 1)+(\pm 1)-(\pm 1) \equiv 0 \pmod{(1-\omega)^4}$ y los posibles valores que podríamos obtener serían $-1, 1, -3, 3$.

Pero $N(\pm 1) = 1$ y $N(\pm 3) = 9$. Por otro lado $N((1-\omega)^4) = N^4(1-\omega) = 3^4 = 81$ y la norma es mayor que la de los dos anteriores.

Podemos suponer que es z quien es divisible por $1-\omega$, ya que la ecuación $x^3 + y^3 = z^3$ es equivalente a las ecuaciones $(-x)^3 + z^3 = y^3$ y $(-y)^3 + z^3 = x^3$. □

Ahora nos disponemos a terminar la demostración de nuestro teorema. Para ello volveremos a utilizar el método del descenso.

De entre todas las soluciones de $x^3 + y^3 = z^3$ donde $1-\omega$ divida a z, elijamos una solución de manera que la potencia de $1-\omega$ que divida a z sea mínima.

Recordemos que

$$(x+y)(\omega x + \omega^2 y)(\omega^2 x \omega y) = x^3 + y^3 = z^3.$$

Como $z^3 \equiv 0 \pmod{1-\omega}$ y $\mathbb{Z}[\omega]$ es un anillo de factorización única, uno de los factores $x+y, \omega x + \omega^2 y, \omega^2 x + \omega y$ es múltiplo de $1-\omega$.

Por otra parte,

$$x + y \equiv \omega x + \omega^2 y \equiv \omega^2 x + \omega y \equiv 0 \pmod{1-\omega}.$$

Entonces

$$\begin{cases} x+y & = (1-\omega)A \\ \omega x + \omega^2 y & = (1-\omega)B \\ \omega^2 x + \omega y & = (1-\omega)C \end{cases}.$$

De la relación $1 + \omega + \omega^2 = 0$ tenemos

$$(x+y) + (\omega x + \omega^2 y) + (\omega^2 x + \omega y) = (1-\omega)(A+B+C) = 0.$$

Seguidamente vamos a ver que $(A,B) = (A,C) = (B,C) = 1$. En efecto si $\gamma \mid (x+y)$ y $\gamma \mid (\omega x + \omega^2 y)$, entonces $\gamma \mid \omega(x+y)$ y $\gamma \mid (\omega x + \omega^2 y)$ y por tanto divide a la diferencia. Es decir $\gamma \mid y(1-\omega^2)$. También $\gamma \mid \omega^2(x+y)$. Restando de nuevo tenemos que $\gamma \mid x(1-\omega^2)$.

Como desde un principio hemos supuesto que $(x,y) = 1$, entonces γ tiene que ser necesariamente $1-\omega$ o uno de sus asociados. Por lo tanto $(A,B) = 1$. De igual manera se demuestra el resto de los casos.

Podemos escribir la ecuación de la forma

$$z^3 = (x+y)(\omega x + \omega^2 y)(\omega^2 x + \omega y) = ABC(1-\omega)^3.$$

Es decir,

$$\left(\frac{z}{1-\omega}\right)^3 = ABC \quad \text{con} \quad (A,B,C) = 1.$$

Como $\mathbb{Z}[\omega]$ es un anillo de factorización única tenemos que

$$A = \alpha\psi^3, \qquad B = \beta\xi^3, \qquad C = \gamma\theta^3,$$

donde α, β, γ son unidades y $\alpha\beta\gamma = \pm 1$.

Como $(x, y, z) = 1$, x e y no pueden ser múltiplos de $1-\omega$; y por el lema 5.2.5, si $x \equiv \pm 1 \pmod{1-\omega}$ entonces $x^3 \equiv \pm 1 \pmod{(1-\omega)^4}$. Igualmente para y.

Tenemos entonces que

$$z^3 = x^3 + y^3 \equiv \pm 1 + \mp 1 \equiv 0 \pmod{(1-\omega)^4}.$$

(Recordemos que $x \equiv y \pmod{1-\omega}$).

Hemos demostrado así que A, B ó C deben ser múltiplos de $1-\omega$. Por ejemplo C.

$$C = \gamma\theta^3 = \gamma(1-\omega)^{3r}\theta_0^3.$$

Supongamos que $(1-\omega)^\lambda$ es la potencia de $1-\omega$ que divide a z. Entonces $3+3r = 3\lambda$ y por lo tanto $r = \lambda - 1$.

De la relación $A + B + C = 0$ tenemos

$$\alpha\psi^3 + \beta\xi^3 + \gamma\left((1-\omega)^{\lambda-1}\theta_0\right)^3 = 0.$$

Y casi hemos llegado a una solución donde el exponente donde el exponente de $1-\omega$ en z es menor que λ. Pero todavía nos estorban α, β y γ.

Como $A = \alpha\psi^3$ y $B = \beta\xi^3$ no son múltiplos de $1-\omega$ entonces $\psi^3 \equiv \pm 1 \pmod{(1-\omega)^4}$ y $\xi^3 \equiv \pm 1 \pmod{(1-\omega)^4}$. De aquí,

$$\alpha\psi^3 + \beta\xi^3 + \gamma\theta^3 \equiv \pm\alpha \pm \beta \equiv 0 \pmod{(1-\omega)^3}.$$

Por otro lado sabemos que $\alpha\beta\gamma = \pm 1$. Como $\alpha = \pm\beta$, entonces $\pm\alpha^2\gamma = \pm 1$. Es decir, $\gamma = \pm\alpha = \pm\beta$.

Dividiendo la ecuación por β, las unidades que nos quedan son 1 ó -1, y ahora sí que las podemos meter dentro del paréntesís para obtener una solución que entra en contradicción con la hipótesis en el método del descenso. □

4.2.4. Representación de enteros como suma de dos cuadrados

En esta sección vamos a estudiar qué enteros son representables como suma de dos cuadrados.

En el capítulo 2 analizamos el comportamiento en media de la función

$$r(n) = \#\{n = a^2 + b^2 : \ a, b \in \mathbb{Z}\}.$$

Concretamente vimos que

$$R(x) = \sum_{n \leq x} r(n) = \pi x + O(\sqrt{x}).$$

Sin embargo ahora vamos a considerar la ecuación $n = x^2 + y^2$ para un n dado y podremos saber el número de soluciones de dicha ecuación en función de la factorización de n en números primos.

Recordemos que el estudio de la factorización de $x^3 + y^3 = z^3$ lo hacíamos en $\mathbb{Z}[\omega]$ porque era allí donde $x^3 + y^3$ se podía factorizar.

No es de extrañar por tanto que el estudio de nuestra ecuación lo hagamos en $\mathbb{Z}[i]$, que es donde se puede factorizar $x^2 + y^2 = (x + iy)(x - iy)$.

Hagamos primeramente una serie de observaciones sobre el anillo $\mathbb{Z}[i] = \{a+bi : a, b \in \mathbb{Z}\}$

1) $N(a + bi) = (a + bi)(a - bi) = a^2 + b^2$.

2) Las unidades de $\mathbb{Z}[i]$ son $\{\pm 1, \pm i\}$.

3) $\mathbb{Z}[i]$ es un anillo euclídeo y por tanto de factorización única.

4) Si $a + bi$ es primo en $\mathbb{Z}[i]$, entonces $a + bi$ divide a un primo racional.

5) Primos en $\mathbb{Z}[i]$. Después de 4), los primos en $\mathbb{Z}[i]$ los podemos buscar entre los divisores de los primos racionales.

   i) $p = 2$.
   Si $N(a + bi) = 2$, entonces $a + bi = 1 + i$ o cualquiera de sus asociados.

   ii) $p \equiv 3 \pmod 4$.
   Si p no fuese primo en $\mathbb{Z}[i]$, existirían a y b tales que $p = (a+bi)(a-bi) = a^2 + b^2$. Pero esto es imposible porque la suma de dos restos cuadráticos módulo 4 nunca puede ser 3.
   Todos los primos $p \equiv 3 \pmod 4$ en $\mathbb{Z}$, son también primos en $\mathbb{Z}[i]$.

a) $p \equiv 1 \pmod 4$.

En el capítulo de la Ley de Reciprocidad cuadrática vimos que si $p \equiv 1 \pmod 4$ entonces -1 era un residuo cuadrático módulo p. Entonces existirá un x tal que $x^2 \equiv -1 \pmod p$. Es decir $p \mid x^2+1 = (x+i)(x-i)$.

Si p fuese primo en $\mathbb{Z}[i]$ debería dividir a alguno de estos factores. Pero ni $x/p + i/p$, ni $x(p - i/p$ son enteros en $\mathbb{Z}[i]$. Luego p tiene que tener algún divisor de la forma $a + bi$; $p = (a + bi)(a - bi) = a^2 + b^2$. Veremos ahora que $a + bi$ es primo en $\mathbb{Z}[i]$.

Si no fuese así tendríamos que $a + bi =)(c + di)(e + fi)$, donde la norma de los factores es mayor que 1. Pero eso es imposible $p = N(a + bi) = N(c + di)N(e + fi)$.

Resumiendo, hemos demostrado que los primos de $\mathbb{Z}[i]$ son $1 + i$, los primos racionales $p \equiv 3 \pmod 4$ y los divisores (que siempre existen) de los primos racionales $p \equiv 1 \pmod 4$.

Teorema 4.2.7. *Si*

$$n = 2^\alpha \prod_{p_j \equiv (4)} p_j^{r_j} \prod_{q_i \equiv 3(4)} q_i^{s_i},$$

entonces

$$r(n) = \begin{cases} 4 \prod_j (1 + r_j) & \textit{si } s_i \textit{ es par para todo } i \\ 0 & \textit{en otro caso.} \end{cases}$$

Demostración. El primer paso será descomponer n en sus factores primos en $\mathbb{Z}[i]$:

$$n = i^t (1 + i)^{2\alpha} \prod_j (a + bi)^{r_j} (a - bi)^{r_j} \prod_i q_i^{s_i}.$$

Buscamos el número de descomposiciones de n de la forma $n = A^2 + B^2 = (A + Bi)(A - Bi)$.

Cada uno de estos factores será de la forma

$$A + Bi = i^{t_1} (1 + i)^{\alpha_1} \prod_j (a + bi)^{r_{j,1}} (a - bi)^{r_{j,2}} \prod_i q_i^{s_{i,1}}$$

$$A - Bi = (-i)^{t_1} (1 - i)^{\alpha_1} \prod_j (a - bi)^{r_{j,1}} (a + bi)^{r_{j,2}} \prod_i q_i^{s_{i,1}}.$$

Igualando normas tenemos que

$$\begin{cases} \alpha_1 & = \alpha \\ r_{j,1} + r_{j,2} & = r_j \\ 2s_{i,1} & = s_i. \end{cases}$$

De aquí se sigue que una condición necesaria para que n sea suma de dos cuadrados es que todos los s_i sean pares.

En ese caso tendremos, para cada j, $r_j + 1$ posibles elecciones de los $r_{j,1}$ y cuatro posibles elecciones de t_1, lo que demuestra el teorema. □

4.2.5. Suma de cuatro cuadrados

Hemos visto que hay números que no se pueden escribir como suma de dos cuadrados y es un ejercicio comprobar que si $n \equiv 7 \pmod 8$ entonces n no se puede escribir como suma de tres cuadrados. ¿Será la suma de cuatro cuadrados suficiente para representar cualquier entero?

Teorema 4.2.8 (Lagrange)**.** *Todo número natural puede expresarse como suma de cuatro cuadrados.*

Demostración. Después del siguiente lema, bastará con demostrar que todo primo p es suma de cuatro cuadrados.

Lema 4.2.9 (Euler)**.** *Si $n = x_1^2 + x_2^2 + x_3^2 + x_4^2$ y $m = y_1^2 + y_2^2 + y_3^2 + y_4^2$, entonces*

$$nm = z_1^2 + z_2^2 + z_3^2 + z_4^2$$

para algunos enteros z_1, z_2, z_3, z_4.

Demostración. Basta con comprobar la relación

$$\begin{aligned}(x_1^2 + x_2^2 + x_3^2 + x_4^2)(y_1^2 + y_2^2 + y_3^2 + y_4^2)\\ = (x_1y_1 + x_2y_2 + x_3y_3 + x_4y_4)^2 + (x_1y_2 - x_2y_1 + x_3y_4 - x_4y_3)^2\\ +(x_1y_3 - x_3y_1 + x_4y_2 - x_2y_4)^2 + (x_1y_4 - x_4y_1 + x_2y_3 - x_3y_2)^2\end{aligned}$$

□

Lema 4.2.10. *Sea p primo impar. Entonces existe un m, $1 \leq m < p$ tal que*

$$mp = x_1^2 + x_2^2 + x_3^2 + x_4^2.$$

Demostración. Consideremos los conjuntos

$$S_1 = \left\{0^2, 1^2, \ldots, \left(\frac{p-1}{2}\right)^2\right\}$$

$$S_2 = \left\{-0^2 - 1, -1^2 - 1, \ldots, -\left(\frac{p-1}{2}\right)^2 - 1\right\}.$$

Los elementos de S_1 son incingruentes entre sí módulo p. En efecto, si $x^2 \equiv y^2 \pmod{p}$ entonces $p \mid (x-y)(x+y)$. Pero eso es imposible porque $0 < x-y < x+y < p$.

Por la misma razón los elementos de S_2 también son incongruentes entre sí. Ambos conjuntos tienen $\frac{p+1}{2}$ elementos. Como entre los dos tienen $p+1$ elementos, dos de ellos, uno de S_1 y otro e S_2, han de ser incongruentes entre sí.

$$x^2 \equiv -y^2 - 1 \pmod{p}.$$

Es decir, $x^2 + y^2 + 1^2 + 0^2 = mp$. Sólo falta por ver que $m < p$. Pero esto sigue de la relación

$$m = \frac{x^2+y^2+1}{p} \leq \frac{(\frac{p-1}{2})^2 + (\frac{p-1}{2})^2 + 1}{p} < p.$$

□

La conclusión del teorema de Lagrange es consecuencia del siguiente lema.

Lema 4.2.11. *Si m es el menor entero que verifica el lema anterior entonces $m = 1$.*

Demostración. Sea m el mínimo entero tal que $mp = x_1^2 + x_2^2 + x_3^2 + x_4^2$. Si m es par tenemos las siguientes posibilidades: todos los x_i son impares, todos los x_i son pares o exactamente dos x_i son pares y los otros dos impares.

En cualquier caso podríamos escribir

$$\frac{m}{2}p = \left(\frac{x_1+x_2}{2}\right)^2 + \left(\frac{x_1-x_2}{2}\right)^2 + \left(\frac{x_3+x_4}{2}\right)^2 + \left(\frac{x_3-x_4}{2}\right)^2.$$

Todos los números en el interior de los paréntesis son enteros, así como $\frac{m}{2}$. Pero entonces $\frac{m}{2}$ verificaría el lema anterior y ya no sería m el mnor número que lo hiciera.

Por lo tanto hemos demostrado que m ha de ser impar. Nuestro objetivo es demostrar que $m = 1$. Vamos a suponer que $m \geq 3$ y llegaremos a una contradicción.

Definamos los y_i de la manera siguiente:

$$y_i \equiv x_i \pmod{m}, \qquad -\frac{m-1}{2} \leq y_i \leq \frac{m-1}{2}.$$

De manera obvia se verifica

$$y_1^2 + y_2^2 + y_3^2 + y_4^2 \equiv x_1^2 + x_2^2 + x_3^2 + x_4^2 \equiv 0 \pmod{m}.$$

Escribamos

$$mn = y_1^2 + y_2^2 + y_3^2 + y_4^2 \leq 4\left(\frac{m-1}{2}\right)^2 < m^2.$$

Es decir, $n < m$.

Si $n = 0$, $y_1 = y_2 = y_3 = y_4 = 0$ y entonces $x_i \equiv 0 \pmod{m}$ y por lo tanto $x_i^2 \equiv 0 \pmod{m^2}$. Luego

$$mp = x_1^2 + x_2^2 + x_3^2 + x_4^2 = km^2$$

y $p = km$ con $1 < m < p$, lo cual es imposible porque p es primo.

Entonces podemos suponer que $n > 0$. Hagamos el siguiente producto utilizando el lema 5.2.9:

$$m^2pn = (x_1^2 + x_2^2 + x_3^2 + x_4^2)(y_1^2 + y_2^2 + y_3^2 + y_4^2) = z_1^2 + z_2^2 + z_3^2 + z_4^2.$$

Como $x_i \equiv y_i \pmod{m}$, tenemos

$$\begin{aligned}
z_2 &\equiv x_1y_2 - x_2y_1 + x_3y_4 - x_4y_3 \\
&\equiv x_1x_2 - x_2x_1 + x_3x_4 - x_4x_3 \equiv 0 \pmod{m} \\
z_3 &\equiv x_1y_3 - x_3y_1 + x_4y_2 - x_2y_4 \\
&\equiv x_1x_3 - x_3x_1 + x_4x_2 - x_2x_4 \equiv 0 \pmod{m} \\
z_4 &\equiv x_1y_4 - x_4y_1 + x_2y_3 - x_3y_2 \\
&\equiv x_1x_4 - x_4x_1 + x_2x_3 - x_3x_2 \equiv 0 \pmod{m} \\
z_1 &\equiv x_1y_1 + x_2y_2 + x_3y_3 + x_4y_4 \\
&\equiv x_1^2 + x_2^2 + x_3^2 + x_4^2 = mp \equiv 0 \pmod{m}
\end{aligned}$$

Ahora podemos escribir

$$pn = \left(\frac{z_1}{m}\right)^2 + \left(\frac{z_2}{m}\right)^2 + \left(\frac{z_3}{m}\right)^2 + \left(\frac{z_4}{m}\right)^2$$

donde los z_i/m son enteros.

Es decir, hemos encontrado un $n < m$ que verifica la hipótesis inicial y contradice el hecho de que m sea el menor entero que la cumple. Por lo tanto hemos completado la demostración. □

□

El teorema de Lagrange es un caso particular del problema de Waring, que consiste en hallar, para cada $k \geq 2$, el menor entero $g(k)$ con la propiedad de que todo entero positivo se puede escribir como suma de $g(k)$ k-potencias. Hilbert demostró que $g(k)$ existe para todo $k \geq 2$ y el teorema de Lagrange demuestra que $g(2) = 4$. Como una aplicación del teorema de Lagrange demostraremos que $g(4) \leq 53$.

Teorema 4.2.12. *Todo entero positivo puede expresarse como suma de* 53 *cuartas potencias.*

Demostración.

Lema 4.2.13.

$$6\left(\sum_{i=1}^{4} x_i^2\right)^2 = \sum_{1\leq i<j\leq 4} (x_i + x_j)^4 + (x_i - x_j)^4.$$

Demostración. Es una simple comprobación. □

EL teorema de Lagrange nos dice que todo número natural se puede escribir como suma de cuatro cuadrados. Luego todo múltiplo de 6 se podrá escribir de la forma $6n_1^2 + 6n_2^2 + 6n_3^3 + 6n_4^2$. Ya cada uno de los sumandos, por el lema anterior, se puede escribir como suma de 12 cuartas potencias. Es decir, todo múltiplo de 6 puede escribirse como suma de 48 cuartas potencias.

Para finalizar, si $n = 6k + r,\ 0 \leq r < 6$, entonces

$$n = 6k + r = \sum_{i=1}^{48} z_i^4 + \sum_{j=1}^{r} 1^4.$$

En el peor de los casos necesitaremos 53 cuartas potencias. □

4.3. Ejercicios del capítulo 4

4.3.1. *Hallar todas las ternas de cuadrados en progresión aritmética.*

4.3.2. *Demostrar que la ecuación* $x^2 + y^2 = 7z^2$ *no tiene soluciones en enteros positivos.*

4.3.3. *Demostrar que si un triángulo rectángulo tiene lados de longitud entera entonces la suma de los lados divide al producto de los mismos.*

4.3.4. *Hallar todas las soluciones enteras de la ecuación* $x^2+y^2 = z^4$ *con* $(x, y, z) = 1$.

4.3.5. *Hallar todas las soluciones en enteros positivos de la ecuación* $\frac{1}{x} + \frac{1}{y} = \frac{1}{z}$.

4.3.6. *Hallar todas las soluciones en enteros positivos de la ecuación* $\frac{1}{x^2} + \frac{1}{y^2} = \frac{1}{z^2}$.

4.3.7. *Demostrar que la ecuación* $\frac{1}{x^4} + \frac{1}{y^4} = \frac{1}{z^2}$ *no tiene soluciones enteras.*

4.3.8. *Probar que* $x^4 + 4y^4 = z^2$ *no tiene soluciones con* $xy \neq 0$.

4.3.9. *Probar que* $x^4 - y^4 = z^2$ *no tiene soluciones con* $yz \neq 0$.

4.3.10. *Hallar todas las soluciones en enteros positivos de la ecuación* $11050 = x^2 + y^2$.

4.3.11. *Demostrar que la única solución en enteros positivos de la ecuación* $y^2 = x^3 - 1$ *es* $y = 3,\ x = 2$.