Reciprocidad y descenso

Ejemplo 1. Si $p = x^2 + y^2$ con $x, y \in \mathbb{Z}$, entonces $p \equiv 1 \pmod 4$, pues $x^2 \equiv 0$ o $x^2 \equiv 1$, dependiendo de si x es par o impar y, si p es un primo impar, x e y deben tener distinta paridad.

Teorema 2. *Un primo impar p se escribe como $x^2 + y^2$ con x e y enteros, si y sólo si $p \equiv 1 \pmod 4$.*

Demostración. Vamos a probar que, si $p \equiv 1 \pmod 4$, entonces existen $x, y \in \mathbb{Z}$ tales que $p = x^2 + y^2$. La demostración estará dividida en dos pasos:

(Descenso) si p divide a una expresión del tipo $a^2 + b^2$ donde $a, b \in \mathbb{Z}$ y $(a, b) = 1$, entonces existen $x, y \in \mathbb{Z}$ tales que $p = x^2 + y^2$;

(Reciprocidad) si $p \equiv 1 \pmod 4$, entonces p divide a algún natural de la forma $a^2 + b^2$ con $a, b \in \mathbb{Z}$ y $(a, b) = 1$.

Probamos cada una de estas afirmaciones, a continuación. □

La idea de Fermat era, aparentemente, la siguiente: si p es primo, $p \equiv 1 \pmod 4$ y p *no* se escribe como suma de dos cuadrados, debería existir un primo $p' < p$ que cumpla que es $p' \equiv 1 \pmod 4$ y que tampoco es suma de dos cuadrados. Eventualmente, llegaríamos a 5 que sí es suma de dos cuadrados. De esta contradicción (de que 5 es y no debería ser suma de dos cuadrados) se deduciría el resultado.

Lema 3. *Sea N un natural que se puede expresar como suma de dos cuadrados* coprimos. *Si q es un divisor primo de N que se puede expresar como suma de dos cuadrados, entonces el cociente también se puede expresar como suma de dos cuadrados coprimos.*

Demostración. Por hipótesis, existen $a, b \in \mathbb{Z}$ tales que $N = a^2 + b^2$ y $(a, b) = 1$ y existen, además, $x, y \in \mathbb{Z}$ tales que $q = x^2 + y^2$ (x e y son, necesariamente, coprimos). Como $q \mid N$, se cumple que q divide a $(bx - ay)(bx + ay)$, pues

$$Nx^2 - a^2q \;=\; b^2x^2 + a^2x^2 - a^2x^2 - a^2y^2 \;=\; (bx)^2 - (ay)^2 \;=\; (bx - ay)\,(bx + ay)\ .$$

Como q es primo, $q \mid bx - ay$, o bien $q \mid bx + ay$. Cambiando el signo de a, podemos suponer que estamos en el primer caso. Esto quiere decir que existe $d \in \mathbb{Z}$ tal que $bx - ay = dq$. Ahora bien,

$$bx - dx^2 \;=\; bx - dq + dy^2 \;=\; ay + dy^2 \;=\; (a + dy)\,y\ .$$

Como $x \mid bx - dx^2$, se cumple que $x \mid (a + dy)y$. Pero $(x, y) = 1$, con lo que $x \mid a + dy$. Existe, entonces, $c \in \mathbb{Z}$ tal que $a + dy = cx$. O sea,

$$a = cx - dy \quad \text{y} \quad b = dx + cy \ .$$

Pero, entonces,

$$N = a^2 + b^2 = (cx - dy)^2 + (dx + cy)^2 = (c^2 + d^2)(x^2 + y^2) = (c^2 + d^2)\, q \ .$$

Así, $N/q = c^2 + d^2$, pero, además, $(a, b) = 1$ implica que $(c, d) = 1$ **(ejercicio)**. $\square$

Observación 4. En la demostración del Lema 3 hicimos uso de la siguiente identidad **(ejercicio)**:

$$(cx - dy)^2 + (dx + cy)^2 = (c^2 + d^2)(x^2 + y^2) \ . \tag{1}$$

Ahora sí, probamos el paso de Descenso.

Lema 5 (Descenso)**.** *Sea p un primo impar que divide a una expresión del tipo $a^2 + b^2$ donde $a, b \in \mathbb{Z}$ y $(a, b) = 1$. Entonces, existen $x, y \in \mathbb{Z}$ tales que $p = x^2 + y^2$.*

Demostración. La hipótesis es que $p \mid N = a^2+b^2$ y $(a, b) = 1$. Veamos, en primer lugar, que podemos asumir, además, que $|a| < p/2$ y que $|b| < p/2$. Cambiando a por $a-kp$ con algún k conveniente, conseguimos $|a-kp| < p/2$. Pero, $(a-kp)^2+b^2 = a^2+b^2-2kp+k^2p^2$. Como $p \mid a^2+b^2$, deducimos que p divide a $(a-kp)^2+b^2$. Cambiamos a por $a-kp$ y ahora p divide a una expresión $a_1^2 + b^2$, donde $|a_1| < p/2$. De la misma manera, conseguimos que p divida una expresión $N_1 := a_1^2 + b_1^2$ con $|b_1| < p/2$. Pero, al hacer estos cambios, podemos haber introducido divisores comunes entre a_1 y b_1. Es decir, puede pasar que $(a_1, b_1) > 1$. Sin embargo, dividiendo por (a_1, b_1), volvemos al caso coprimo. Veamos esto. Sea $d := (a_1, b_1)$. Por cómo fueron elegidos $a_1 = a - kp$ y $b_1 = b - lp$ con $k, l \in \mathbb{Z}$. Como $(a, b) = 1$, en particular, p no es un divisor común de a y de b. Pero, entonces, p tampoco es un divisor común de a_1 y de b_1. O sea, $(p, d) = 1$. De esta manera, si $N_2 := N_1/d^2$, $a_2 := a_1/d$ y $b_2 := b_1/d$, entonces $a_2, b_2 \in \mathbb{Z}$, $|a_2| \leq |a_1| < p/2$ y $|b_2| \leq |b_1| < p/2$, $(a_2, b_2) = 1$ y, finalmente, $p \mid N_2$ (aquí usamos que $(p, d) = 1$).

Recapitulando, asumimos que $p \mid N$, donde $N = a^2 + b^2$, $(a, b) = 1$, $|a| < p/2$ y $|b| < p/2$. Bajo estas suposiciones adicionales, $N < p^2/2$. En particular, si $q \neq p$ es un divisor primo de N, debe ser $q < p$. Separamos dos casos: o bien todo tal q es suma de dos cuadrados, o bien existe un divisor primo q de N que no es suma de cuadrados. En el primer caso, por el Lema 3, se deduce, eliminando todos los factores primos distintos de p, que p también debe ser suma de cuadrados (notar que $p^2 \nmid N$). Supongamos, para llegar a una contradicción que p no es suma de cuadrados. Entonces, existiría un divisor primo de N, $q < p$, que tampoco es suma de cuadrados. Necesariamente, q debe ser impar ($2 = 1^2 + 1^2$) y, más aun, $q \equiv 1 \pmod 4$.[1] Pero, entonces, estaríamos en las mismas hipótesis del resultado que queremos probar: q es primo impar que divide a

[1] Si $q \mid a^2 + b^2$, con $(a, b) = 1$, entonces $a^2 + b^2 \equiv 0 \pmod q$ y $-1 \equiv (ab^{-1})^2 \pmod q$. Es decir, existe $x \in \mathbb{Z}$ tal que $x^4 \equiv 1 \pmod q$, pero $x^2 \not\equiv 1 \pmod q$. Esto implica que $4 \mid \varphi(q) = q-1$, o sea, $q \equiv 1 \pmod 4$.

$N = a^2 + b^2$, con la diferencia de que q es estrictamente más chico que p. Eventualmente, deberíamos llegar al menor primo con esta propiedad. Para terminar, notamos que el menor primo impar congruente con 1 módulo 4 es 5 que sí es suma de cuadrados ($5 = 2^2 + 1^2$). Llegamos a la siguiente contradicción 5 es suma de cuadrados, pero, por el proceso por el que *descendimos* hasta este primo, 5 no debería ser suma de cuadrados. Esta contradicción viene de suponer que el primo p del cual partimos no era suma de cuadrados. $\square$

Lema 6 (Reciprocidad)**.** *Si p es un número primo impar y $p \equiv 1 \pmod 4$, entonces p divide a una expresión del tipo $a^2 + b^2$ donde $a, b \in \mathbb{Z}$ y $(a, b) = 1$.*

Demostración. Por hipótesis, $p - 1 = 4k$, $k \in \mathbb{Z}$, entonces, como $\varphi(p) = p - 1$, $x^{4k} \equiv 1 \pmod p$, para todo $x \in \mathbb{Z}$ coprimo con p (o sea, para todo $x \not\equiv 0 \pmod p$), o, lo que es lo mismo, $p \mid x^{4k} - 1$. Pero $x^{4k} - 1 = (x^{2k} - 1)(x^{2k} + 1)$. Como p es primo, $p \mid x^{2k} - 1$ o bien $p \mid x^{2k} + 1$. En términos de congruencias, para todo $x \in \mathbb{Z}$, $(x, p) = 1$,

$$x^{2k} - 1 \equiv 0 \pmod p \quad \text{o bien} \quad x^{2k} + 1 \equiv 0 \pmod p .$$

Es decir, cada una de las $p - 1$ clases de congruencia $\not\equiv 0$ módulo p es solución de alguna de estas dos ecuaciones de congruencia. Pero, como $2k < p$, existe $x \in \mathbb{Z}$ tal que $x^{2k} - 1 \not\equiv 0 \pmod p$ **(ejercicio)**.[2] Entonces, debe ser $x^{2k} + 1 \equiv 0 \pmod p$. Obtenemos el resultado eligiendo $a = x^k$ y $b = 1$. $\square$

[2] La cantidad de raíces módulo p es, a lo sumo, el grado del polinomio.