Teorema navideño de Fermat

Benjamín Macías Quezada

Fue Albert Girard quien identificó los enteros positivos—no necesariamente primos—que se pueden escribir como sumas de cuadrados de enteros [Ste25], pero la clasificación de los primos que son sumas de cuadrados fue conjeturada por Fermat cuarenta años después en una carta a Mersenne fechada un 25 de diciembre:

Teorema 1 (Fermat, 1640). *Un número primo impar es suma de dos cuadrados de números enteros si y solo si es congruente a* 1 *módulo* 4

Una de las implicancias es una cuenta directa: supongamos que $p \in \mathbb{Z}$ es un primo impar, y que es igual a una suma de cuadrados de números enteros. Los residuos cuadráticos módulo 4 son solo 0 y 1, por lo que dicha suma solo puede ser $0, 1$, o 2 módulo 4. Como p es impar, la suma no puede ser 0 ni 2 módulo 4, lo que deja solo la posibilidad de que sea 1 módulo 4. La otra implicancia es la no-trivial.

Existen múltiples demostraciones conocidas de la implicancia restante. Entre ellas, hay dos de Euler usando descenso infinito [Eul58, Eul60], otra de Lagrange mediante formas cuadráticas [Lag75] (que es un refinamiento de un argumento de Gauß [Gau01, art. 182]), otras gracias a Heath-Brown–Zagier [Zag90, HB84] (que se hizo popular por consistir en una sola oración). En nuestro caso, nos va a interesar una demostración elemental de Dedekind, que aparece en sus *Vorlesungen über Zahlentheorie* [Ded71], que utiliza los enteros gaussianos y un poco de teoría de Euclides.

Recordemos que el anillo de los *enteros gaussianos* es el conjunto

$$\mathbb{Z}[i] := \{a + bi \colon a, b \in \mathbb{Z}\},$$

equipado con la suma y producto usuales de $\mathbb{C}$. Es un dominio euclidiano respecto a la norma $N(a+bi) := a^2 + b^2$ (que es una función multiplicativa), y por tanto un dominio de factorización única.

La gracia de trabajar en $\mathbb{Z}[i]$ es que, en contraste a $\mathbb{Z}$, las sumas de cuadrados se pueden factorizar: un cálculo directo muestra que $a^2 + b^2 = (a + bi)(a - bi)$. Con esto en mente, podemos demostrar el resultado:

Demostración del Teorema. Sea $p \in \mathbb{Z}$ primo de la forma $p = 1 + 4n$ para algún $n \in \mathbb{N}$. Notemos que para demostrar la implicancia restante basta probar que p no es un primo en $\mathbb{Z}[i]$: en este caso se tendrá una factorización $p = \alpha\beta$ como producto de no-unidades de $\mathbb{Z}[i]$, y al tomar norma, obtenemos la igualdad $p^2 = N(\alpha)N(\beta)$. En tanto α, β no son unidades, su norma es distinta de 1, por lo que la igualdad anterior fuerza que $p^2 = N(\alpha)^2$ y por tanto que $p = N(\alpha)$. Escribiendo $\alpha = a + bi$ para algunos $a, b \in \mathbb{Z}$, se exhibe que $p = a^2 + b^2$.

Para verificar que p no es primo en $\mathbb{Z}[i]$, vamos a probar que

$$p \mid x^2 + 1 = (x + i)(x - i)$$

para algún $x \in \mathbb{Z}[i]$, pero que no divide a ninguno de estos factores. La primera parte es equivalente, por definición, a resolver la congruencia

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

en $\mathbb{Z}[i]$, lo que será posible con un poco de manipulación algebraica y el Teorema de Wilson. En primer lugar, notamos que

$$\begin{aligned}
(p-1)! = (4n)! &= \prod_{k=1}^{2n} k \prod_{k=2n+1}^{4n} k \\
&= (2n)! \prod_{k=1}^{2n} (k + 2n) \\
&= (2n)! \prod_{k=1}^{2n} (k - 1 + 2n + 1) \\
&= (2n)! \prod_{k=1}^{2n} (k - 1 + p - 2n) \\
&\equiv (2n)! \prod_{k=1}^{2n} (k - 1 - 2n) \pmod{p} \\
&= (2n)!(-1)^{2n} \prod_{k=1}^{2n} (2n + 1 - k) \\
&= (2n)! \cdot (2n)! = [(2n)!]^2.
\end{aligned}$$

Por el Teorema de Wilson, se tiene que $-1 \equiv (p-1)! \pmod{p}$, por lo que $x_n := (2n)!$ es una solución de la ecuación 1. Por tanto, $p \mid (x_n + i)(x_n - i)$.

Para checkear que p no divide a $(x_n + i)(x_n - i)$, basta notar que esto implicaría que x_n/p o $\pm i/p$ son elementos de $\mathbb{Z}[i]$, lo que no es posible. Así, p no es un primo de $\mathbb{Z}[i]$, y concluimos lo deseado por lo discutido inicialmente. □

Referencias

[Ded71] Richard Dedekind, *Vorlesungen über zahlentheorie*, Vieweg, Braunschweig, Germany, 1871.

[Eul58] Euler, Leonhard, *De numerus qui sunt aggregata quorum quadratorum*, Novi commentarii academiae scientiarum Petropolitanae **4** (1758), 3–40.

[Eul60] ———, *Demonstratio theorematis fermatiani omnem numerum primum formae 4n+1 esse summam duorum quadratorum*, Novi commentarii academiae scientiarum Petropolitanae **5** (1760), 3–13.

[Gau01] Carl Friedrich Gauss, *Disquisitiones arithmeticae*, In commissis libraria Schäferi, Gottingae, 1801.

[HB84] Roger Heath-Brown, *Fermat's two squares theorem*, journalId:00001884 **11** (1984).

[Lag75] Joseph-Louis Lagrange, Nouv. Mém. Acad. Berlin (1775), 351.

[Ste25] Simon Stevin, *l'Arithmétique de Simon Stevin de Bruges*, Leyde, 1625, Annotated by Albert Girard.

[Zag90] D. Zagier, *A one-sentence proof that every prime* $p \equiv 1$ (mód 4) *is a sum of two squares*, The American Mathematical Monthly **97** (1990), no. 2, 144.