Suma de cuadrados y teorema de Fermat

Daniel Campos Salas

(Material en construcción)

Contents

1 Introducción **1**

2 Bézout, inversos multiplicativos y Wilson **2**

3 Prueba de las observaciones: idea del descenso **3**

4 Tópicos avanzados: polinomios sobre cuerpos **5**

5 Problemas **5**

6 ¿Qué sigue después? **6**

1 Introducción

Vamos a realizar observaciones en el siguiente experimento. Consideramos la sucesión de cuadrados perfectos $\{0, 1, 4, 9, 16, \ldots\}$ y la sumamos consigo mismo:

	1	4	9	16	25	36	49
1	2	5	10	17	26	37	50
4	$*$	8	13	20	29	40	53
9	$*$	$*$	18	25	34	45	58
16	$*$	$*$	$*$	32	41	52	65
25	$*$	$*$	$*$	$*$	50	61	74
36	$*$	$*$	$*$	$*$	$*$	72	85
49	$*$	$*$	$*$	$*$	$*$	$*$	98

¿Qué fenómenos podemos notar en la tabla? Una primera observación puede ser la siguiente.

Observación 1. *Si m pertenece a la tabla, entonces $2m$ también.*

Prueba. Si m pertenece a la tabla, entonces sabemos que existen enteros a y b tales que $m = a^2 + b^2$. Necesitamos demostrar que $2m^2$ también se escribe como una suma de dos cuadrados perfectos. En efecto, esto se sigue al reescribir

$$2m^2 = 2a^2 + 2b^2 = (a^2 - 2ab + b^2) + (a^2 + 2ab + b^2) = (a - b)^2 + (a + b)^2.$$

□

Si analizamos con cuidado algunos de los números que aparecen en la tabla, como

$$10 = 2 \cdot 5, \quad 26 = 2 \cdot 13, \quad 34 = 2 \cdot 17, \quad 40 = 5 \cdot 8, \ldots,$$

podemos generalizar la observación anterior de la siguiente manera.

Observación 2. *Si m y n pertenecen a la tabla, entonces mn también.*

Prueba. Suponemos que $m = a^2 + b^2$ y $n = c^2 + d^2$, de manera que

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

Tenemos que reescribir la expresión como una suma de dos cuadrados, lo cual podemos lograr mediante

$$mn = (a^2c^2 - 2abcd + b^2d^2) + (a^2d^2 + 2abcd + b^2c^2) = (ac - bd)^2 + (ad + bc)^2,$$

que es lo que queríamos probar. □

Relacionado con el análisis anterior de casos particulares, la siguiente observación va a consistir en el "centro" de todo el desarrollo posterior que hagamos.

Observación 3. *Si un número primo p divide a un número de la tabla y p^2 no lo divide, entonces el primo p aparece en la tabla.*

Esta observación no es tan sencilla de demostrar y nos ocupará el resto del desarrollo. Ya que detuvimos nuestra atención en los números primos, podemos hacer una lista de los números primos que aparecen en la lista:

$$2,\ 5,\ 13,\ 17,\ 29,\ 37,\ 41,\ 53,\ 61, \ldots.$$

En la lista total de primos, podemos resaltar los que aparecen en la lista:

$$\mathbf{2},\ 3,\ \mathbf{5},\ 7,\ 11,\ \mathbf{13},\ \mathbf{17},\ 19,\ 23,\ \mathbf{29},\ 31,\ \mathbf{37},\ \mathbf{41},\ 47, \ldots.$$

Hay varias observaciones que podemos hacer al respecto.

Observación 4. *Ningún primo de la forma $4k+3$ aparece en la tabla. Es más, ningún número $4k+3$ aparece en la tabla.*

Prueba. Buscamos los residuos cuadráticos módulo 4:

a	0	± 1	2
a^2	0	1	0

Es decir, los residuos cuadráticos son $\{0, 1\}$. Por lo tanto, no es posible obtener un número de la forma $4k + 3$ como suma de dos cuadrados. □

En la dirección de Observación 3, y complementando a Observación 4, podemos hacer una observación mucho menos trivial.

Observación 5. *Todos los primos de la forma $4k + 1$ aparecen en la tabla.*

2 Bézout, inversos multiplicativos y Wilson

En el proceso de demostración de Observación 3 y Observación 5 es necesario desviarnos (en apariencia) momentáneamente de lo que estábamos estudiando.

Teorema 2.1 (Bézout)**.** *Sean a y b enteros positivos, y sea $d = (a, b)$. Entonces, existen enteros m y n tales que $am + bn = d$.*

Comentario. *Es claro que el máximo común divisor d divide a cualquier combinación lineal $am+bn$; el teorema lo que afirma es que la combinación lineal "óptima" se puede alcanzar.*

Prueba. Algoritmo euclidiano, PENDIENTE. □

Corolario 2.2. *Si a y b son enteros positivos coprimos, entonces a tiene un inverso multiplicativo módulo b; es decir, existe c tal que $ac \equiv 1$ (mód b). Además, este inverso es único módulo b.*

Prueba. En esta prueba vamos a considerar todas las congruencias módulo b. Por Teorema 2.1 sabemos que existen enteros c y d tales que $ac + bd = 1$, lo cual implica que $ac \equiv 1$.

Si c_1 y c_2 son enteros tales que $ac_1 \equiv ac_2 \equiv 1$, entonces obtenemos que $c_1 \equiv c_1(ac_2) \equiv ac_1c_2$ y también $c_2 \equiv c_2(ac_1) \equiv ac_1c_2$, por lo que concluimos que $c_1 \equiv c_2$, es decir, el inverso es único módulo b. □

Corolario 2.3. *Si p es un primo y $1 \leq a < p$, entonces existe $1 \leq b < p$ tal que $ab \equiv 1$ (mód p).*

Ejemplo. *Para $p = 7$, la lista de inversos multiplicativos es la siguiente:*

a	1	2	3	4	5	6
a^{-1}	1	4	5	2	3	6

es decir,

a	$\pm$ 1	$\pm$ 2	$\pm$ 3
a^{-1}	$\pm$ 1	$\mp$ 3	$\mp$ 2

Ejercicio. *Encuentre la lista de inversos multiplicativos para otro número primo.*

La experiencia de los ejemplos anteriores nos conducen hacia la prueba del siguiente teorema

Teorema 2.4 (Wilson)**.** *Si p es un número primo, entonces $(p-1)! \equiv -1$ (mód p).*

Prueba. Para $p = 2$ el resultado es obvio, por lo que solo vamos a considerar el caso en que p es impar. La idea de la prueba consiste en agrupar los factores $\{1, 2, \ldots, p-1\}$ en parejas de inversos multiplicativos. El ejemplo (y el ejercicio) sugieren que solo $\{1, p-1\}$ son su propio inverso multiplicativo; vamos a demostrar esto. Si k es su propio inverso multiplicativo, entonces $k^2 \equiv 1$ (mód p). Esto implica que p divide a $k^2 - 1 = (k-1)(k+1)$, y como p es primo, entonces p divide a $k-1$ o a $k+1$, es decir $k = 1$ o $k = p-1$. Por lo tanto, podemos separar los factores de $(p-1)!$ en $\{1, p-1\}$ y los grupos de parejas de inversos multiplicativos. Siguiendo el ejemplo de arriba, esto consistiría en agrupar $7!$ de la forma $1 \cdot 6 \cdot (2 \cdot 4) \cdot (3 \cdot 5)$. Por lo tanto, $(p-1)! \equiv 1 \cdot (p-1) \equiv -1$ (mód p), como queríamos probar. □

Más adelante, daremos una demostración alternativa (y tal vez más natural) del teorema anterior.

3 Prueba de las observaciones: idea del descenso

El teorema de Wilson implica el siguiente resultado importante relacionado con las observaciones hechas al inicio.

Teorema 3.1. *Si p es un primo de la forma $4k + 1$, entonces existe un entero a tal que p divide a $a^2 + 1$. Es decir, -1 es un residuo cuadrático módulo p.*

Prueba. En esta prueba consideramos las congruencias módulo p. Si $p = 4k + 1$, entonces podemos escribir

$$(p-1)! = [1 \cdot 2 \cdot \ldots \cdot (2k)] \cdot [(2k+1) \cdot \ldots \cdot (4k)] \equiv (2k)! \cdot (-2k) \cdot \ldots \cdot (-1) = (-1)^{2k}[(2k)!]^2 = [(2k)!]^2.$$

Finalmente, el resultado se sigue de Teorema 2.4. □

Motivados teorema anterior y Observación 3 procedemos a demostrar el siguiente proposición, propuesto en la IMO Shortlist 1978, [1].

Proposición 3.2. *Sean x, y, z enteros no negativos tales que $xy = z^2 + 1$. Entonces existen enteros a, b, c, d tales que*

$$x = a^2 + b^2, \quad y = c^2 + d^2, \quad z = ac + bd, \quad |ad - bc| = 1.$$

Antes de proceder con la demostración de la proposición, es bueno hacer casos particulares e intentar entender mejor la proposición. Una forma sencilla de generar casos particulares es asignando valores a z, con lo que x y y quedan determinados (en vez de asignarlos a x y y):

z	x	y	a	b	c	d
0	1	1	1	0	0	1
1	2	1	1	1	1	0
2	5	1	2	1	1	0
3	10	1	3	1	1	0
3	5	2	2	1	1	1

Prueba. La idea de la prueba es reemplazar una terna (x, y, z) por otra $(\widetilde{x}, \widetilde{y}, \widetilde{z})$, de manera que la nueva sea "más pequeña" en algún sentido y aplicar inducción sobre esto. Empezamos notando que, excepto en el caso en que $z = 0$, siempre vamos a tener $x \neq y$; sin pérdida de generalidad podemos asumir que $x > y > 0$. Tenemos entonces que

$$x^2 > xy = z^2 + 1 > z^2, \quad y^2 < xy = z^2 + 1 \leq (z+1)^2,$$

por lo que $x > z$ y $y < z + 1$, es decir, $z \geq y$. Además, si $y = z$, entonces z divide a $xy - z^2 = 1$, lo cual solo es posible cuando $z = 1$. Es decir, si $z > 1$ entonces tenemos que $x > z > y$. Podemos construir una nueva terna al considerar

$$(z-y)^2 + 1 = (z^2+1) - 2yz + y^2 = xy - 2yz + y^2 = (x + y - 2z)y,$$

es decir, tomando $(\widetilde{x}, \widetilde{y}, \widetilde{z}) = (x + y - 2z, y, z - y)$. Una forma de cuantificar que esta terna es más pequeña que (x, y, z) es observando que $\widetilde{z} < z$. Es decir, podemos usar inducción sobre z. Los casos básicos los realizamos antes. Ahora, por hipótesis inductiva tenemos que

$$x + y - 2z = \widetilde{x} = a^2 + b^2, \quad y = \widetilde{y} = c^2 + d^2, \quad z - y = \widetilde{z} = ac + bd, \quad |ad - bc| = 1.$$

Esto implica que

$$z = (ac + bd) + y = ac + bd + c^2 + d^2 = (a + c)c + (b + d)d,$$

$$x = (a^2 + b^2) - y + 2z = (a^2 + b^2) - (c^2 + d^2) + 2(ac + bd + c^2 + d^2) = (a + c)^2 + (b + d)^2.$$

Tomando $A = a + c$, $B = b + d$, $C = c$, $D = d$, obtenemos que

$$x = A^2 + B^2, \quad y = C^2 + D^2, \quad z = AC + BD, \quad |AD - BC| = 1,$$

lo que completa la tesis inductiva. □

La prueba de Observación 5 se sigue directamente de Teorema 3.1 y Proposición 3.2. Nos falta demostrar solamente Observación 3. Supongamos que p divide a $a^2 + b^2$, pero p^2 no divide a $a^2 + b^2$. Si $d = (a, b)$, con $a = dA$ y $b = dB$, entonces $a^2 + b^2 = d^2(A^2 + B^2)$. Como p^2 no divide a $a^2 + b^2$, entonces p no divide a d (pues d^2 divide a $a^2 + b^2$); por lo tanto, tenemos que p divide a $A^2 + B^2$ con $(A, B) = 1$. Por Teorema 2.1 sabemos que existen C y D tales que $AC + BD = 1$. Por lo tanto p divide a

$$(A^2 + B^2)(C^2 + D^2) = (AD - BC)^2 + (AC + BD)^2 = E^2 + 1.$$

Por Proposición 3.2 esto implica que p se puede escribir como una suma de cuadrados, es decir, p pertenece a la tabla.

4 Tópicos avanzados: polinomios sobre cuerpos

En esta sección damos una prueba alternativa más robusta del teorema de Wilson y usamos el resultado para demostrar otros resultados adicionales.

Primero introducimos un poco de notación para hacer más sencillo el desarrollo. Dado un entero positivo N, denotamos por $\mathbb{Z}/N\mathbb{Z}$ el conjunto de residuos módulo N. Este conjunto tiene suma (con inversos aditivos y elemento neutro) y producto (con elemento neutro), por lo que lo llamamos un **anillo**.

Ejemplo. *Los enteros y los polinomios con coeficientes reales (en una o más variables) son ejemplos de anillos.*

Sea p un número primo. Por Corolario 2.3 tenemos que todo elemento no nulo de $\mathbb{Z}/p\mathbb{Z}$ tiene un inverso multiplicativo. Esta es una propiedad muy especial y por lo tanto decimos que este anillo es un **cuerpo**.

Ejemplo. *Otros ejemplos de cuerpos son los números racionales, los reales y los complejos.*

No-ejemplo. *Los enteros y los polinomios con coeficientes reales no son cuerpos, porque hay elementos que no tienen inversos multiplicativos.*

Ejercicio. *Demuestre que si $\mathbb{Z}/N\mathbb{Z}$ es un cuerpo, entonces N tiene que ser primo. Es decir, si N no es primo, encuentre un residuo no nulo en $\mathbb{Z}/N\mathbb{Z}$ que no tenga inverso multiplicativo.*

Al igual que con los polinomios con coeficientes reales, tenemos que si k es un cuerpo, entonces podemos considerar polinomios con coeficientes en k. El siguiente resultado generaliza el hecho que un polinomio con coeficientes reales de grado d no puede tener más de d raíces (contadas con multiplicidad).

Proposición 4.1. *Un polinomio no nulo, de grado d y con coeficientes en un cuerpo k, no puede tener más de d raíces (contadas con multiplicidad).*

Ejercicio. *La condición de tener los coeficientes en un cuerpo es fundamental. Demuestre que en $\mathbb{Z}/4\mathbb{Z}$ el polinomio lineal $p(x) = 2x$ tiene dos raíces.*

Ahora estamos listos para dar una demostración alternativa del teorema de Wilson. Consideramos los polinomios mónicos (es decir, que su coeficiente principal es 1) de grado $p-1$:

$$f(x) = (x-1)(x-2)\dots(x-(p-1)), \qquad g(x) = x^{p-1} - 1.$$

Claramente, $f(1) = f(2) = \ldots = f(p-1) = 0$. Además, por estar trabajando sobre $\mathbb{Z}/p\mathbb{Z}$, por el pequeño teorema de Fermat tenemos que $g(1) = g(2) = \ldots = g(p-1) = 0$. Podemos considerar la diferencia $h(x) = f(x) - g(x)$ y obtener que $h(1) = h(2) = \ldots = h(p-1) = 0$. Sin embargo, h es un polinomio de grado menor que $p-1$, pues los dos coeficientes principales de f y g se cancelan. Si h no es el polinomio nulo, entonces Proposición 4.1 da una contradicción. Por lo tanto, h debe ser el polinomio nulo, lo que implica que los coeficientes respectivos de f y g son iguales en $\mathbb{Z}/p\mathbb{Z}$, es decir, los coeficientes son congruentes módulo p. En particular, el último coeficiente de $f(x)$ es $(-1)^{p-1}(p-1)! = (p-1)!$ (si $p \geq 3$) y por lo tanto $(p-1)! \equiv -1$ (mód p).

Polinomios simétricos y sumas de potencias. PENDIENTE.

5 Problemas

Ejercicio. *Como en la prueba de Observación 2, demuestre la desigualdad de Cauchy-Schwarz,*

$$(a_1^2 + \ldots + a_n^2)(b_1^2 + \ldots + b_n^2) \geq (a_1 b_1 + \ldots + a_n b_n)^2,$$

escribiendo la diferencia como una suma de cuadrados.

Ejercicio. *Escriba $a^2 + b^2 = (a + bi)(a - bi)$ y combine los factores en el producto, para dar una demostración alternativa de Observación 2.*

Ejercicio. *Vamos a dar una demostración alternativa de Teorema 3.1 para p un primo impar. En este ejercicio vamos a considerar todas las congruencias módulo p. Denotamos por $\mathbb{Z}/p\mathbb{Z}$ el conjunto de residuos módulo p y por $(\mathbb{Z}/p\mathbb{Z})^*$. el conjunto de residuos invertibles módulo p. Por Corolario 2.3 sabemos que $(\mathbb{Z}/p\mathbb{Z})^* = \mathbb{Z}/p\mathbb{Z} \setminus \{0\}$. Para $n \in (\mathbb{Z}/p\mathbb{Z})$ denotamos por n^{-1} a su inverso multiplicativo. Consideramos el conjunto*

$$\mathcal{S} := \{n + n^{-1} : n \in (\mathbb{Z}/p\mathbb{Z})^*\}.$$

1. *Demuestre que $m + m^{-1} \equiv n + n^{-1}$ si y sólo si $m \equiv n$ o $m \equiv n^{-1}$.*
2. *Demuestre que el conjunto $\mathcal{S}$ tiene $(p + 1)/2$ elementos.*
3. *Demuestre que si $s \in \mathcal{S}$, entonces $-s \in \mathcal{S}$; es decir, existe una función $\varphi : \mathcal{S} \to \mathcal{S}$ que satisface $\varphi(\varphi(s)) = s$ para todo $s \in \mathcal{S}$.*
4. *Demuestre que si $\Phi : X \to X$ es una función que satisface $\Phi(\Phi(x)) = x$ para todo x y X tiene un número impar de elementos, entonces Φ tiene un punto fijo; es decir, existe $x_0 \in X$ tal que $\Phi(x_0) = x_0$.*
5. *Deduzca que si $p = 4k + 1$, entonces $\varphi : \mathcal{S} \to \mathcal{S}$ tiene un punto fijo.*
6. *Concluya que -1 es un residuo cuadrático módulo p si $p = 4k + 1$.*

Ejercicio. *En Teorema 3.1 demostramos que si p es un primo de la forma $4k + 1$ entonces -1 es un residuo cuadrático. Demuestre que si p es un primo de la forma $4k + 3$, entonces -1 **no** es un residuo cuadrático. (Sugerencia: si $p = 4k + 3$, use el pequeño teorema de Fermat y que $(p - 1)/2 = 2k + 1$ es impar.)*

Problema 1 (Entrenamiento Singapur, IMO 2003)**.** *Demuestre que existen infinitos puntos con coordenadas racionales en el círculo unitario $x^2 + y^2 = 1$, tales que la distancia entre cualesquiera par de puntos es irracional.*

Problema 2 (IMOSL 1997)**.** *Sea p un número primo y f un polinomio con coeficientes enteros, de grado d, con $f(0) = 0$, $f(1) = 1$ y $f(n) = 0$ o 1 módulo p para todos los enteros n. Pruebe que $d \geq p - 1$.*

Problema 3 (K. Česnavičius, IMO 2008, Problema 3)**.** *Demuestre que existen infinitos enteros positivos n tales que $n^2 + 1$ tiene un divisor primo mayor que $2n + \sqrt{2n}$.*

6 ¿Qué sigue después?

1. Unicidad en la representación.
2. Reciprocidad cuadrática.
3. Enteros gaussianos y dominios de factorización única (tópicos avanzados).
4. Primos de la forma $x^2 + ny^2$ [2].
5. Teorema de los cuatro cuadrados de Lagrange (cuaterniones?).

References

[1] D. Djukić, et al., *The IMO Compendium*, Problem Books in Mathematics, Springer, 2006.

[2] D.A. Cox, *Primes of the form $x^2 + ny^2$. Fermat, Class Field Theory, and Complex Multiplication*, Pure and Applied Mathematics, John Wiley & Sons, 2013.