El Pequeño Teorema de Fermat

Por Carlos Jacob Rubio Barrios

Nivel Intermedio

Pierre de Fermat (1601-1665), era un concejal de la Audiencia Provincial de la Judicatura en Toulouse, al sur de Francia, que practicaba las matemáticas en su tiempo libre. Sus resultados los comunicaba a sus amigos a través de cartas, y al final resultó que sus obras influyeran significativamente en el desarrollo de la matemática moderna.

En la época de Fermat se tenía la siguiente "hipótesis china":

$$p \text{ es un número primo si y sólo si } 2^p \equiv 2 \pmod{p}.$$

En un sentido la hipótesis no es verdadera. En efecto, el número $2^{341} - 2$ es divisible entre 341, y $341 = 11 \times 31$ no es primo. Sin embargo, la otra dirección de la hipótesis es verdadera. A partir de los manuscritos y las cartas de Fermat se sabe que Fermat conocía (y lo más probable sabía la demostración) de los siguientes hechos:

1. Si n no es primo, entonces $2^n - 1$ no es primo.
2. Si n es primo, entonces $2^n - 2$ es múltiplo de $2n$.
3. Si n es primo y p es un divisor primo de $2^n - 1$, entonces $p - 1$ es múltiplo de n.

El primer enunciado se puede demostrar directamente al factorizar $2^n - 1$. En efecto, si $n = ab$, con $a > 1$ y $b > 1$, entonces,

$$\begin{aligned} 2^n - 1 &= 2^{ab} - 1 \\ &= (2^a - 1)(2^{a(b-1)} + 2^{a(b-2)} + \cdots + 1). \end{aligned}$$

Los otros dos enunciados son variaciones del siguiente resultado más general, indicado en otra de sus cartas: Dado un número primo p, y cualquier progresión geométrica

$1, a, a^2, \ldots$, el número p debe dividir a algún número $a^n - 1$ con n divisor de $p-1$; luego, si N es cualquier múltiplo del menor de tales números n para los cuales se cumple lo anterior, entonces p divide también a $a^N - 1$.

En notación de congruencias, podemos reescribir el enunciado anterior de la siguiente manera, y al que nos referiremos como pequeño teorema de Fermat: *Si p es un número primo y a es cualquier entero, entonces $a^p \equiv a \pmod p$. En particular, si p no divide al entero a, entonces $a^{p-1} \equiv 1 \pmod p$.*

Fermat no publicó ninguna demostración del pequeño teorema de Fermat, y fue Leonard Euler (1707-1783) quien primero lo hizo por inducción.

Cuatro demostraciones del pequeño teorema de Fermat

El resultado es claro si $p = 2$. Así que asumiremos que $p > 2$. Observemos que si p es un primo impar, basta demostrar el resultado para $a > 0$ ya que si $a = -b \leq 0$, entonces $a^p \equiv (-b)^p \equiv -b^p \equiv -b \equiv a \pmod p$.

1. Primera demostración. Supongamos que $p \nmid a$ y demostremos que $a^{p-1} \equiv 1 \pmod p$. Consideremos los enteros $a, 2a, \ldots, (p-1)a$. Si tuviéramos que $ai \equiv aj \pmod p$ para ciertos enteros i, j, tales que $1 \leq i \leq p-1$ y $1 \leq j \leq p-1$, tendríamos que $p \mid a(i-j)$ y $p \mid i-j$, de donde $i = j$. Luego, los residuos de estos números son $1, 2, \ldots, p-1$ en algún orden y por lo tanto,

$$a(2a)\cdots(p-1)a \equiv 1 \cdot 2 \cdots (p-1) \pmod p,$$

es decir,

$$a^{p-1}(p-1)! \equiv (p-1)! \pmod p.$$

Como p y $(p-1)!$ son primos relativos, podemos dividir ambos lados de la congrencia anterior entre $(p-1)!$ (ver [2]) y por lo tanto $a^{p-1} \equiv 1 \pmod p$.

2. Segunda demostración. Procederemos por inducción en a. Si $a = 1$ el resultado es inmediato. Supongamos que el resultado es cierto para algún entero $k > 1$. Aplicando el teorema del binomio, tenemos que:

$$(k+1)^p \quad = \quad \sum_{j=0}^{p} \binom{p}{j} k^{p-j} = k^p + \sum_{j=1}^{p-1} \binom{p}{j} k^{p-j} + 1.$$

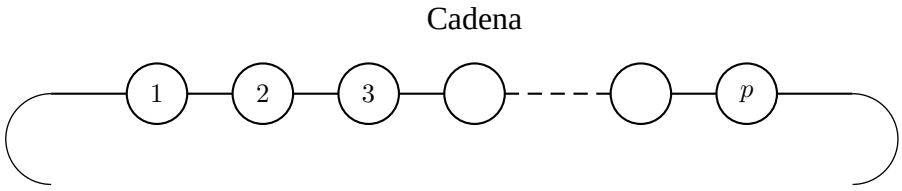
Como $\binom{p}{j} \equiv 0 \pmod p$ para $1 \leq j \leq p-1$ (ejercicio), tenemos que $(k+1)^p \equiv k^p + 1 \pmod p$ y por la hipótesis de inducción se sigue que $(k+1)^p \equiv k+1 \pmod p$. Por lo tanto, $a^p \equiv a \pmod p$ para todo entero positivo a.
Finalmente, $(a, p) = 1$ y $a(a^{p-1} - 1) \equiv 0 \pmod p$ implican que $a^{p-1} \equiv 1 \pmod p$.

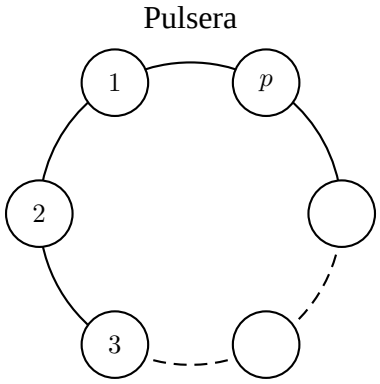
3. Tercera demostración. La haremos mediante un argumento combinatorio. Queremos demostrar que $a^p - a$ es múltiplo de p. Esto es equivalente a demostrar que el

resultado de dividir $a^p - a$ entre p es un entero. Vamos a demostrar esto al establecer que esta fracción es igual al número de elementos en un conjunto particular, y por lo tanto debe ser un entero.

Supongamos que tenemos cuentas que vienen en a colores. Queremos seleccionar p de estas cuentas para formar una cadena con ellas. Está permitido repetir colores. Ya que estamos usando p cuentas, y cada una de ellas puede ser de cualquiera de los a colores, tenemos a^p secuencias de colores diferentes. Como es aburrido tener todas las cuentas del mismo color, pediremos que al menos se utilicen dos colores. Tenemos a cadenas en las cuales todas las cuentas son del mismo color. Restando estas del total, obtenemos $a^p - a$ cadenas en las cuales al menos se utilizan dos colores distintos.

Ahora vamos a unir los extremos de cada cadena para formar una pulsera. Cuando esto se hace, algunas de nuestras cadenas se vuelven indistinguibles. Por ejemplo, supongamos que sólo estuviéramos usando tres cuentas. Cuando las ponemos en una línea recta, la cadena con cuentas "verde, azul, naranja" parece distinta de la cadena con cuentas "azul, naranja, verde". Pero si unimos los extremos de cada cadena, obtendríamos dos pulseras indistinguibles.





Ahora nos preguntamos: "De las $a^p - a$ pulseras que usan al menos dos colores, ¿cuántas de ellas son indistinguibles entre sí?" La respuesta es que cada cadena de p cuentas puede ser cambiada cíclicamente sin producir una pulsera distinta. En nuestro ejemplo, las cadenas:

verde, azul, naranja;
azul, naranja, verde;
naranja, verde, azul;

todas se verán como la misma pulsera cuando los extremos de cada una estén unidos. Ya que cada uno de los p corrimientos cíclicos de una cadena dada nos genera pulseras indistinguibles, tenemos que el número de pulseras indistinguibles que usan al menos dos colores es igual a $\frac{a^p-a}{p}$, y como el número de tales pulseras es un entero, el resultado queda probado.

Ahora nos preguntamos en qué parte del argumento anterior usamos que p es un número primo. La respuesta está en el paso donde afirmamos que cada cadena dada se cuenta p diferentes veces, una por cada uno de los cambios cíclicos posibles. Esto es cierto para un número primo, pero no es cierto en general. Por ejemplo, supongamos que usamos seis cuentas y comenzamos con la cadena,

verde, azul, azul, verde, azul, azul.

Si movemos cíclicamente todas las cuentas una vez, obtenemos la cadena,

azul, azul, verde, azul, azul, verde,

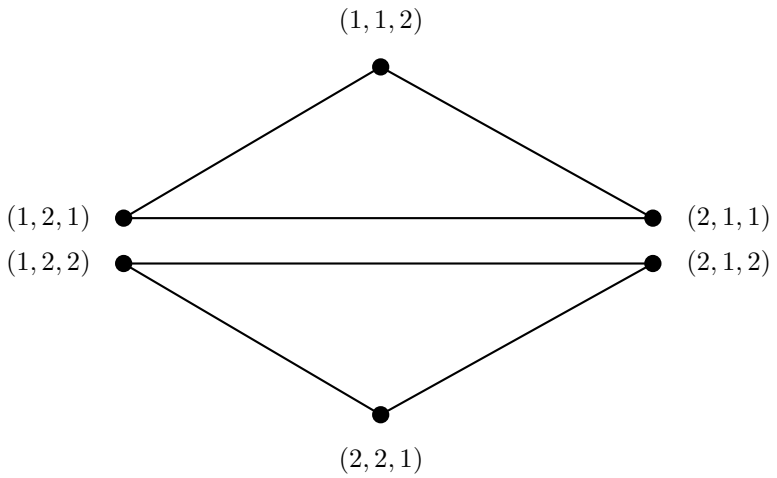
la cual nos dará la misma pulsera. Sin embargo, un cambio más nos lleva a la cadena,

verde, azul, azul, verde, azul, azul,

que es precisamente la cadena con la que comenzamos. En este caso sólo hay 3 cadenas que nos llevan a pulseras indistinguibles de la original. Esto es precisamente el tipo de situación que no puede suceder si estamos usando un número primo de cuentas.

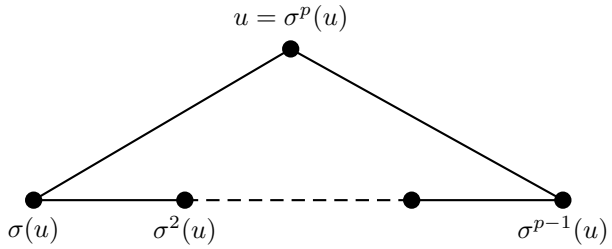
La tercera demostración se puede reescribir utilizando conceptos de teoría de grafos, como lo veremos a continuación en la cuarta y última demostración. Se recomienda al lector consultar la definición 2 en el apéndice.

4. Cuarta demostración. Consideremos el grafo G donde el conjunto de vértices V es el conjunto de todas las p-tuplas $(u_1, u_2, \ldots, u_p)$ de enteros positivos entre 1 y a (inclusive) con $u_i \neq u_j$ para algunos $i \neq j$. Es claro que V tiene $a^p - a$ elementos. Dado $u \in V$, $u = (u_1, u_2, \ldots, u_p)$, diremos que uv es una arista de G si y sólo si $v = \sigma(u) = (u_p, u_1, \ldots, u_{p-1})$.
Por ejemplo, si $a = 2$ y $p = 3$, tenemos el siguiente grafo.



El grafo G para $a = 2$ y $p = 3$

Consideremos un vértice arbitrario $u = (u_1, u_2, \ldots, u_p)$ de G. Este vértice es adyacente con los vértices $\sigma(u) = (u_p, u_1, \ldots, u_{p-1})$ y $\sigma^{p-1}(u) = (u_2, u_3, \ldots, u_p, u_1)$, donde $\sigma^i(u) = \sigma^{i-1}(\sigma(u))$ para $i = 2, 3, \ldots$.
Observemos que $\sigma(u) \neq \sigma^{p-1}(u)$, pues en caso contrario, tendríamos que $u_p = u_2, u_1 = u_3, \ldots, u_{p-2} = u_p, u_{p-1} = u_1$, de donde $u_1 = u_3 = u_5 = \cdots = u_{p-1}$ y $u_2 = u_4 = \cdots = u_p$. Luego, el vértice u sería una p-tupla de la forma $u = (a, b, a, b, \ldots, a, b)$ lo cual no puede ser porque p es un primo impar y en este caso u tiene un número par de coordenadas. Por lo tanto, cada vértice de G es adyacente a 2 vértices distintos y en consecuencia, G es una unión disjunta de ciclos (ejercicio para el lector).



Demostraremos que cada uno de estos ciclos tiene longitud igual a p. Supongamos que $u = (u_1, u_2, \ldots, u_p)$ pertenece a un ciclo de longitud $t < p$. Entonces, $\sigma^t(u) = u$ y tenemos también que $\sigma^p(u) = u$. Por el algoritmo de la división podemos escribir $p = tq + r$ para algunos enteros q y r con $0 \leq r < t$, de modo que $u = \sigma^p(u) = \sigma^{tq+r}(u) = \sigma^r(u)$. Luego, si $0 < r < t$ tendríamos que u está en un ciclo de longitud menor que t lo cual es una contradicción. Por lo tanto, $r = 0$ y de aquí $t \mid p$. Como p es primo, se sigue que $t = 1$ o $t = p$. La igualdad $t = 1$ no puede suceder porque cada vértice es adyacente a dos vértices distintos. Por lo tanto, $t = p$ y así G está formado por ciclos disjuntos de longitud p. De estos es fácil ver que hay $\frac{a^p - a}{p}$ y por lo tanto $a^p \equiv a \pmod{p}$.

Aplicaciones

A continuación veremos algunas aplicaciones del pequeño teorema de Fermat en la solución de problemas de olimpiada.

1. Si a es un entero positivo, demostrar que cualquier factor primo mayor que 2 del número a^2+1 es de la forma $4m+1$.

Solución. Sea p un factor primo mayor que 2 del número a^2+1 y supongamos que p no es de la forma $4m+1$. Entonces, p es de la forma $p=4m+3$ para algún entero m. Entonces $a^2 \equiv -1 \pmod{p}$ y

$$a^{p-1} \equiv (a^2)^{2m+1} \equiv (-1)^{2m+1} \equiv -1 \pmod{p},$$

lo que contradice el pequeño teorema de Fermat.

2. Determinar todas las soluciones en enteros x, y que satisfacen la ecuación,

$$1998^2x^2 + 1997x + 1995 - 1998x^{1998} = 1998y^4 + 1993y^3 - 1991y^{1998} - 2001y.$$

Solución. Demostraremos que la ecuación no tiene soluciones en enteros. Supongamos que (x,y) es una solución. Como 1997 es primo, aplicando el pequeño teorema de Fermat tenemos que $x^{1997} \equiv x \pmod{1997}$ y $y^{1997} \equiv y \pmod{1997}$. Luego, $x^{1998} \equiv x^2 \pmod{1997}$ y $y^{1998} \equiv y^2 \pmod{1997}$. Considerando la ecuación del problema módulo 1997 tenemos que,

$$x^2 + 0 - 2 - x^2 \equiv y^4 - 4y^3 + 6y^2 - 4y \pmod{1997},$$

la cual se simplifica en

$$-1 \equiv (y-1)^4 \pmod{1997}. \tag{1}$$

En particular, $y-1$ es primo relativo con 1997. Aplicando nuevamente el pequeño teorema de Fermat, tenemos que $(y-1)^{1996} \equiv 1 \pmod{1997}$.
Por otro lado, la congruencia en (1) implica que $(-1)^{499} \equiv (y-1)^{4(499)} \pmod{1997}$, es decir, $-1 \equiv (y-1)^{1996} \pmod{1997}$, lo que es una contradicción.

3. (Olimpiada Rioplatense, 2004) Hallar el número de enteros $n > 1$ tales que el número $a^{13} - a$ sea divisible entre n para todo entero positivo a.

Solución. Sea $n > 1$ un entero tal que $a^{13} - a$ es divisible entre n para todo entero positivo a. Tenemos que p^2, con p primo, no divide a n, ya que p^2 no divide a $p^{13} - p$. Luego, n es producto de primos distintos. Como n debe dividir al número $a^{13} - a$ para todo entero a, en particular n debe dividir al número $2^{13} - 2 = 2 \cdot 3^2 \cdot 5 \cdot 7 \cdot 13$. El pequeño teorema de Fermat implica que $a^{13} \equiv a \pmod{p}$ para $p = 2, 3, 5, 7$ y 13, y por lo tanto $a^{13} \equiv a \pmod{2 \cdot 3 \cdot 5 \cdot 7 \cdot 13}$ para todo entero a. Luego, los enteros

$n > 1$ que cumplen el problema son precisamente los divisores positivos distintos de 1 del número $2 \cdot 3 \cdot 5 \cdot 7 \cdot 13$. Por lo tanto, la respuesta es $2^5 - 1 = 31$ enteros.

4. (Olimpiada Internacional, 2005) Consideremos la sucesión $a_1, a_2, \ldots$ definida por $a_n = 2^n + 3^n + 6^n - 1$ para $n = 1, 2, \ldots$. Determinar todos los enteros positivos que son primos relativos con cada término de la sucesión.

Solución. Sea $p > 3$ un número primo. Por el pequeño teorema de Fermat, tenemos que,

$$3 \cdot 2^{p-1} + 2 \cdot 3^{p-1} + 6^{p-1} \equiv 6 \pmod{p}.$$

Luego, podemos dividir la congruencia anterior entre 6 obteniendo,

$$2^{p-2} + 3^{p-2} + 6^{p-2} \equiv 1 \pmod{p},$$

es decir, p divide al término a_{p-2} de la sucesión. Además, es claro que 2 divide a a_1 y 3 divide a a_2. Por lo tanto, el único número que es primo relativo con cada término de la sucesión es el 1.

5. (Olimpiada Mexicana, 2010) Sean p, q, r números primos distintos. Demostrar que si pqr divide a,

$$(pq)^r + (qr)^p + (rp)^q - 1,$$

entonces $(pqr)^3$ divide a,

$$3((pq)^r + (qr)^p + (rp)^q - 1).$$

Solución. Sin pérdida de generalidad supongamos que $p > q > r$. Vamos a encontrar todas las ternas de números primos (p, q, r) que cumplan que $pqr \mid (pq)^r + (qr)^p + (rp)^q - 1$. Sea (p, q, r) una terna que cumple lo anterior. Como $p \mid (pq)^r$ y $p \mid (rp)^q$, tenemos que $p \mid (qr)^p - 1$, es decir, $(qr)^p \equiv 1 \pmod{p}$. Por otro lado, por el pequeño teorema de Fermat, tenemos que $(qr)^p \equiv qr \pmod{p}$. Luego, $qr \equiv 1 \pmod{p}$, es decir, $p \mid qr - 1$. Análogamente, tenemos que $q \mid rp - 1$ y $r \mid pq - 1$. Entonces, $pq + pr + qr - 1$ es divisible entre p, q y r, así que, $pq + pr + qr - 1 \equiv 0 \pmod{pqr}$, de donde, $pqr + 1 \leq pq + pr + qr$.
Demostraremos que $r = 2$. Supongamos que $r \geq 3$. Ya que $pq > pr$ y $pq > qr$, tenemos que,

$$pqr + 1 > pqr \geq 3pq > pq + pr + qr,$$

lo cual es una contradicción. Por lo tanto, $r = 2$.
Sustituyendo tenemos que $2pq \mid 2q + 2p + pq - 1$, luego $pq \mid 2(p + q) - 1$, de donde $pq + 1 \leq 2(p + q)$.
Demostraremos ahora que $q = 3$. Supongamos que $q \geq 5$, entonces $pq + 1 > pq \geq 5p > 2(p+q)$, lo cual es una contradicción. Por lo tanto, $q = 3$. Si volvemos a sustituir obtenemos que $6p \mid 5 + 5p$, luego $6p \leq 5 + 5p$ y así $p \leq 5$. Como p es primo y $p > q = 3$, concluimos que $p = 5$.
Por lo tanto, si (p, q, r) cumple que $p > q > r$ son números primos tales que pqr divide

a $(pq)^r + (qr)^p + (rp)^q - 1$, entonces $p = 5$, $q = 3$ y $r = 2$.
Si demostramos que $5^3 3^3 2^3 \mid 3((5 \cdot 3)^2 + (3 \cdot 2)^5 + (2 \cdot 5)^3 - 1)$ habremos terminado. Observemos que,

$$\begin{aligned} 2^3 &\mid (15^2 - 1) + 6^5 + 10^3 \\ 3^2 &\mid 15^2 + 6^5 + (10^3 - 1) \\ 5^3 &\mid (15^2 + 6^5 - 1) + 10^3. \end{aligned}$$

Luego, $5^3 3^2 2^3 \mid 15^2 + 6^5 + 10^3 - 1$, de donde

$$5^3 3^3 2^3 \mid 3((5 \cdot 3)^2 + (3 \cdot 2)^5 + (2 \cdot 5)^3 - 1).$$

A continuación se dejan unos ejercicios para el lector.

Ejercicios

1. Para cada entero $n \geq 0$, sea $a_n = 2^{3n} + 3^{6n+2} + 5^{6n+2}$. Determina el máximo común divisor de los números $a_0, a_1, a_2, \ldots, a_{2012}$.

2. Demuestra que para cualquier número primo p, el número $p^{p+1} + (p+1)^p$ no es un cuadrado.

3. Determina todos los enteros positivos n tales que $7 \mid 2^n - 1$.

4. Demuestra que $7 \nmid 2^n + 1$ para todo entero positivo n.

5. Sean a y b enteros positivos tales que $a > b$ y $a + b$ es par. Demuestra que las raíces de la ecuación,

$$x^2 - (a^2 - a + 1)(x - b^2 - 1) - (b^2 + 1)^2 = 0$$

son enteros positivos tales que ninguno de ellos es un cuadrado.

6. Demuestra que $n \nmid 2^{n-1} + 1$ si n es un entero mayor que 1.

7. Determina todos los números primos p y q tales que $pq \mid 2^p + 2^q$.
(Sugerencia: Usa el ejercicio anterior.)

Bibliografía

1. T. Andreescu, D. Andrica. *Number Theory: Structures, Examples and Problems.* Birkhäuser, 2009.

2. A. Rechtman Bulajich, C. J. Rubio Barrios. *Divisibilidad y congruencias.* Revista de la Olimpiada Mexicana de Matemáticas, *Tzaloa*, No. 2, 2009.