TEORÍA ELEMENTAL DE NÚMEROS

DAVID M. BURTON, TRADUCIDO POR PAUL A. LOOMIS

5.2 El Pequeño Teorema de Fermat y los Seudoprimos

El corresponsal más significativo de Fermat en la teoría de números fue Bernhard Frénicle de Bessy (1605-1675), un funcionario en la casa de moneda francesa que era famoso por su don de manipular números grandes. (La facilidad de Frénicle en el cálculo numerical se revela en el siguiente incidente: Al escuchar que Fermat había propuesta el problema de encontrar cubos que, cuando aumentado por sus propios divisores se convierten en cuadrados, como es el caso con $7^3+(1+7+7^2) = 20^2$, inmediatamente se dio cuatros soluciones distintas, y produjo seis más el día siguiente.) Aunque de ninguna manera el igual de Fermat como matemático, el único Frénicle entre sus contemporáneos podía desafiar a Fermat en la teoría de números y los desafíos de Frénicle tuvo la distinción de sacarle a Fermat sus secretos más cuidadosamente guardados. Uno de los más llamativos es el teorema que establece: Si p es un primo y a es cualquier número entero no divisible por p, entonces p divide a $a^{p-1} - 1$. Fermat comunicó el resultado en una carta del 18 de octubre 1640, junto con el comentario "Le enviaría la demostración, si no temiera que fuera demasiada larga." Desde entonces se conoce este teorema como el "Pequeño Teorema de Fermat", para distinguirlo del "Gran" o "Último Teorema" de Fermat, lo que es el tema del Capitulo 12. Pasaron casi 100 años antes de Euler publicó la primera demostración del teorema pequeña en 1736. Aunque parece que Leibniz no ha recibido su parte del reconocimiento, porque dejó un argumento idéntico en un manuscrito no publicado en algún momento antes de 1683.

Ahora procedemos a una demostración del teorema de Fermat.

Teorema 5.1. Teorema de Fermat Sea p un primo y supongamos que $p \nmid a$. Entonces $a^{p-1} \equiv 1 \pmod{p}$.

Demostracion: Comenzamos considerando los primeros $p-1$ multiples de a; es decir, los enteros

$$a, 2a, 3a, \ldots, (p-1)a$$

Ningunos de estos números es congruente moódulo p a ningún otro, y ninguno es congruente a cero. De hecho, si pasaría que

$$ra \equiv sa \pmod{p} \qquad 1 \leq r < s \leq p-1$$

entonces se podría cancelar para obtener $r \equiv s \pmod{p}$, que es imposible. Por lo tanto, el conjunto anterior de enteros debe ser congruente módulo p a $1, 2, 3, \ldots, p-$

1, en algún orden. Multiplicando todos estas congruencias juntos, encontramos que

$$a \cdot 2a \cdot 3a \cdots (p-1)a \equiv 1 \cdot 2 \cdot 3 \cdots \cdot (p-1) \pmod{p}$$

por lo cual

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

Al cancelar $(p-1)!$ de ambos lados de la congruencia anterior (esto es posible como $p \nmid (p-1)!$), nuestra linea de razonamiento culmina en la declaración que $a^{p-1} \equiv 1 \pmod{p}$, que es el teorema de Fermat.

Se puede declarar este resultado de una manera un poco más general en que se elimina el requisito que $p \nmid a$.

Corolario. Si p es un primo, entonces $a^p \equiv a \pmod{p}$ para cualquier entero a.

Demostración: Cuando $p|a$, la declaración obviamente es valida; como, en esta configuración, $a^p \equiv 0 \equiv a \pmod{p}$. Si $p \nmid a$, entonces según el teorema de Fermat, tenemos $a^{p-1} \equiv 1 \pmod{p}$. Cuando se multiplica esta congruencia por a, la conclusión $a^p \equiv a \pmod{p}$ sigue.

Hay una demostración distinta del hecho que $a^p \equiv a \pmod{p}$ involucrando la inducción en a. Si $a = 1$, la afirmación es que $1^p \equiv 1 \pmod{p}$, que claramente es cierto, como es el caso $a = 0$. Suponiendo que el resultado es cierto para a, debemos confirmar su validez para $a + 1$. A la luz del teorema del binomio,

$$(a+1)^p = a^p + \binom{p}{1}a^{p-1} + \cdots + \binom{p}{k}a^{p-k} + \cdots + \binom{p}{p-1}a + 1$$

en donde la coeficiente está dado por

$$\binom{p}{k} = \frac{p!}{k!(p-k)!} = \frac{p(p-1)\cdots(p-k+1)}{1 \cdot 2 \cdot 3 \cdots k}$$

Nuestro argumento gira en torno a la observación que $\binom{p}{k} \equiv 0 \pmod{p}$ para $1 \leq k \leq p-1$. Para ver esto, nota que

$$k!\binom{p}{k} = p(p-1)\cdots(p-k+1) \equiv 0 \pmod{p}$$

de donde $p|k!$ o $p|\binom{p}{k}$. Pero $p|k!$ implica que $p|j$ por algún j que satisface $1 \leq j \leq k \leq p-1$, que es absurdo. Por lo tanto, $p|\binom{p}{k}$, o, convirtiendo a una declaración de congruencia,

$$\binom{p}{k} \equiv 0 \pmod{p}$$

El punto que deseamos señalar es que

$$(a+1)^p \equiv a^p + 1 \equiv a + 1 \pmod{p}$$

en que la congruencia más a la derecha usa nuestra hipótesis de inducción. Entonces, la conclusión deseada es cierta para $a+1$ y en consecuencia para cada $a \geq 0$. Si pasa que a es un entero negativo, no hay problema; como $a \equiv r \pmod{p}$ para algún r, en donde $0 \leq r \leq p-1$, obtenemos $a^p \equiv r^p \equiv r \equiv a \pmod{p}$.

El teorema de Fermat tiene muchas aplicaciones y es central a mucho de lo que se hace en la teoría de números. En lo mínimo, puede ser un dispositivo que ahorre trabajo en ciertos cálculos. Si se le pide que verifique que $5^{38} \equiv 4 \pmod{11}$, por ejemplo, tomamos la congruencia $5^{10} \equiv 1 \pmod{11}$ como nuestro punto de partida. Sabiendo esto,

$$\begin{aligned} 5^{38} = 5^{10\cdot 3+8} &= (5^{10})^3(5^2)^4 \\ &\equiv 1^3 \cdot 3^4 \equiv 81 \equiv 4 \pmod{11} \end{aligned}$$

como se desee.

Otro uso del teorema de Fermat es como herramienta para probar la primalidad de un entero dado n. Si se pudiera demostrar que la congruencia

$$a^n \equiv a \pmod{n}$$

no se cumple por alguna elección de a, entonces n es necesariamente compuesto. Como ejemplo de este enfoque, veamos el $n = 117$. La computación se controla por seleccionar un pequeño entero para a, digamos $a = 2$. Como se puede escribir 2^{117} como

$$2^{117} = 2^{7\cdot 16+5} = (2^7)^{16}2^5$$

y $2^7 = 128 \equiv 11 \pmod{117}$, tenemos

$$2^{117} \equiv 11^{16} \cdot 2^5 \equiv (121)^8 2^5 \equiv 4^8 \cdot 2^5 \equiv 2^{21} \pmod{117}$$

Pero $2^{21} = (2^7)^3$, lo que lleva a

$$2^{21} \equiv 11^3 \equiv 121 \cdot 11 \equiv 4 \cdot 11 \equiv 44 \pmod{117}$$

Al combinar estas congruencias, en fin obtenemos

$$2^{117} \equiv 44 \not\equiv 2 \pmod{117}$$

de modo que 117 debe ser compuesto; de hecho, $117 = 13 \cdot 9$.

Podría valer la pena dar un ejemplo que ilustra el fracaso del reciproco del teorema de Fermat de mantenerse cierto. Como preludio requerimos un lema técnico.

Lema. Si p y q son primos distintos con $a^p \equiv a \pmod{q}$ y $a^q \equiv a \pmod{p}$, entonces $a^{pq} \equiv a \pmod{pq}$.

Demostración. El último corolario nos dice que $(a^q)^p \equiv a^q \pmod{p}$, mientras $a^q \equiv a \pmod{p}$ es cierta por hipótesis. Al combinar estas congruencias, obtenemos $a^{pq} \equiv a \pmod{p}$ o, en otros términos, $p | a^{pq} - a$. En una manera completamente similar, $q | a^{pq} - a$. El Corolario 2 al Teorema 2.4 produce $pq | a^{pq} - a$, que puede reformularse como $a^{pq} \equiv a \pmod{pq}$.

Nuestra argumento es que $2^{340} \equiv 1 \pmod{341}$ en donde $341 = 11 \cdot 31$. En trabajar hacía este fin, nota que $2^{10} = 1024 = 31 \cdot 33 + 1$. Entonces,

$$2^{11} = 2 \cdot 2^{10} \equiv 2 \cdot 1 \equiv 2 \pmod{31}$$

y

$$2^{31} = 2(2^{10})^3 \equiv 2 \cdot 1^3 \equiv 2 \pmod{11}$$

Explotando el lema,

$$2^{11 \cdot 31} \equiv 2 \pmod{11 \cdot 31}$$

o $2^{341} \equiv 2 \pmod{341}$. Después de cancelar un factor de 2, pasamos a

$$2^{340} \equiv 1 \pmod{341}$$

de modo que el reciproco al teorema de Fermat es falso.

El interés histórico en los números de la forma $2^n - 2$ reside en la afirmación hecho por los matemáticos chinos hace más que 25 siglos de que n es primo si y solo si $n|2^n - 2$ (de hecho, este criterio es válido para todos los enteros $n \leq 340$). Nuestro ejemplo, en donde $341|2^{341} - 2$, aunque $341 = 11 \cdot 31$, pone fin a la conjetura; esto fue descubrido en el año 1819. La situación en que $n|2^n - 2$ ocurre con suficiente frecuencia como para merecer un nombre; un entero compuesto se llama *seudoprimo* siempre que $n|2^n - 2$. Se puede demostrar que hay infinitos seudoprimos, los cuatro más pequeño siendo 341, 561, 645, y 1105.

El Teorema 5.2 nos permite construir una secuencia creciente de seudoprimos.

Teorema 5.2. Si n es un seudoprimo impar, entonces $M_n = 2^n - 1$ es uno más grande.

Demostración: Como n es un número compuesto, podemos escribir $n = rs$, con $1 < r \leq s < n$. Luego, según el Problema 21 de Sección 2.3, $2^r - 1|2^n - 1$, o equivalentemente $2^r - 1|M_n$, haciendo M_n compuesto. Por nuestros hipóteses, $2^n \equiv 2 \pmod{n}$; entonces $2^n - 2 = kn$ por algún entero k. Resulta que

$$2^{M_n - 1} = 2^{2^n - 2} = 2^{kn}$$

Esto produce

$$\begin{aligned} 2^{M_n - 1} &= 2^{kn} - 1 \\ &= (2^n - 1)(2^{n(k-1)} + 2^{n(k-2)} + \cdots + 2^n + 1) \\ &= M_n(2^{n(k-1)} + 2^{n(k-2)} + \cdots + 2^n + 1) \\ &\equiv 0 \pmod{M_n} \end{aligned}$$

Vemos inmediatamente que $2^{M_n} - 2 \equiv 0 \pmod{M_n}$, en visto de lo cual M_n es un seudoprimo.

Más generalmente, un entero compuesto n para que $a^n \equiv a \pmod{n}$ se llama un *seudoprimo a la base a* (Cuando $a = 2$, n simplemente se llama un seudoprimo.) Por ejemplo, 91 es el mínimo seudoprimo a la base 3, mientras 217 es el mínimo tal

a la base 5. Ha sido demostrado (1903) que hay infinitos seudoprimos a cualquier base dada.

Estos "primos impostores" son mucho más raros que los primos reales. En efecto, hay solo 247 seudoprimos menores que un millón, en comparación con 78498 primos. El primer ejemplo de un seudoprimo par, a saber, el número

$$161038 = 2 \cdot 73 \cdot 1103$$

fue encontrado en 1950.

Existen números compuestos n que son seudoprimos a toda base a; es decir, $a^{n-1} \equiv 1 \pmod{n}$ para cada entero n con $\text{mcd}(a, n) = 1$. El más pequeño tal es 561. Estos números excepcionales se llaman *seudoprimos absolutos* o *números de Carmichael*, para R. D. Carmichael, quien fue el primero de notar su existencia. En su primer artículo en el tema, publicado en 1910, Carmichael indicó cuatro seudoprimos absolutos incluyendo el bien conocido $561 = 3 \cdot 11 \cdot 17$. Los otros son $1105 = 5 \cdot 13 \cdot 17$, $2821 = 7 \cdot 13 \cdot 31$, y $15841 = 7 \cdot 31 \cdot 73$. Dos años después se presentó 11 más teniendo tres factores primos y descubrió un seudoprimo absoluto con cuatro factores, específicamente, $16046641 = 13 \cdot 37 \cdot 73 \cdot 457$.

Para ver que $561 = 3 \cdot 11 \cdot 17$ debe ser un seudoprimo absoluto, nota que $\text{mcd}(a, 561) = 1$ da

$$\text{mcd}(a, 3) = \text{mcd}(a, 11) = \text{mcd}(a, 17) = 1$$

Una aplicación del teorema de Fermat conduce a las congruencias

$$a^2 \equiv 1 \pmod{3} \qquad a^{10} \equiv 1 \pmod{11} \qquad a^{16} \equiv 1 \pmod{17}$$

y, a su vez, a

$$\begin{aligned} a^{560} &\equiv (a^2)^{280} \equiv 1 \pmod{3} \\ a^{560} &\equiv (a^{10})^{56} \equiv 1 \pmod{11} \\ a^{560} &\equiv (a^{16})^{35} \equiv 1 \pmod{17} \end{aligned}$$

Estas dan lugar a la congruencia única $a^{560} \equiv 1 \pmod{561}$, en donde $\text{mcd}(a, 561) = 1$. Pero entonces $a^{561} \equiv a \pmod{561}$ para cada a, demostrando que 561 es un seudoprimo absoluto.

Cada seudoprimo absoluto es libre de cuadrados. Esto es fácil demostrar. Supongamos que $a^n \equiv a \pmod{n}$ para cada entero a, pero $k^2 | n$ para algún $k > 1$. Si dejamos que $a = k$, entonces $k^n \equiv k \pmod{n}$. Como $k^2 | n$, esta última congruencia es cierta módulo k^2; es decir, $k \equiv k^n \equiv 0 \pmod{k^2}$, y por consiguiente $k^2 | k$, lo cual es imposible. Entonces, n debe ser libre de cuadrados.

A continuación presentamos un teorema que proporciona un medio para producir seudoprimos absolutos.

Teorema 5.3. Sea n un entero positivo y libre de cuadrados, digamos $n = p_1 p_2 \cdots p_r$, en donde los p_i son primos distintos. Si $p_i - 1 | n - 1$ para $i = 1, 2, \ldots, r$, entonces n es un seudoprimo absoluto.

Demostración: Supongamos que a es un entero que satisface $\text{mcd}(a, n) = 1$, de modo que $\text{mcd}(a, p_i) = 1$ para cada i. Entonces el teorema de Fermat produce $p_i | a^{p_i - 1} - 1$. Del hipótesis de divisibilidad $p_i - 1 | n - 1$, tenemos $p_i | a^{n-1} - 1$ y por lo tanto $p_i | a^n - a$ para cada a y $i = 1, 2, \ldots, r$. Como resultado del Corolario 2 del Teorema 2.4, obtenemos $n | a^n - a$, lo que convierte a n un seudoprimo absoluto.

Ejemplos de enteros que satisfacen las condiciones del Teorema 5.3 son

$$1729 = 7 \cdot 13 \cdot 19 \qquad 6601 = 7 \cdot 23 \cdot 41 \qquad 10585 = 5 \cdot 29 \cdot 73$$

Fue demostrado en 1994 que existen infinitos seudoprimos absolutos, pero que son bastante raros. Solo hay 43 de ellos menor que un millón, y 105212 menos que 10^{15}.

PROBLEMAS 5.2

1. Usar el teorema de Fermat para verificar que 17 divide a $11^{104} + 1$.

2. a) Si $\text{mcd}(a, 35) = 1$, demostrar que $a^{12} \equiv 1 \pmod{35}$.
[Consejo: Del Teorema de Fermat, $a^6 \equiv 1 \pmod 7$ y $a^4 \equiv 1 \pmod 5$.]
b) Si $\text{mcd}(a, 42) = 1$, demostrar que $168 = 3 \cdot 7 \cdot 8$ divide a $a^6 - 1$.
c) Si $\text{mcd}(a, 133) = \text{mcd}(b, 133) = 1$, demostrar que $133 | a^{18} - b^{18}$.

3. Del Teorema de Fermat deducir que, para cada entero $n \geq 0$, $13 | 11^{12n+6} + 1$.

4. Derivar cada una de las consecuencias siguientes:
a) $a^{21} \equiv a \pmod{15}$ para cada a.
[Consejo: Por el Teorema de Fermat, $a^5 \equiv a \pmod 5$.]
b) $a^7 \equiv a \pmod{42}$ para cada a.
c) $a^{13} \equiv a \pmod{3 \cdot 7 \cdot 13}$ para cada a.
d) $a^9 \equiv a \pmod{30}$ para cada a.

5. Si $\text{mcd}(a, 30) = 1$, demostrar que 60 divide a $a^4 + 59$.

6. a) Hallar el dígito de las unidades de 3^{100} por el uso del Teorema de Fermat.
b) Para cualquier entero a, verificar que a^5 y a contienen el mismo dígito de unidades.

7. Si $7 \nmid a$, demostrar que o $a^3 + 1$ o $a^3 - 1$ es divisible por 7.

8. Las tres apariciones más recientes del cometa Halley fueron en los años 1835, 1910, y 1986; la próxima ocurrencia será en 2061. Demostrar que

$$1835^{1910} + 1986^{2061} \equiv 0 \pmod 7$$

9. a) Sea p un primo y $\text{mcd}(a, p) = 1$. Usar el Teorema de Fermat para verificar que $x \equiv a^{p-2} b \pmod p$ es una solución a la congruencia lineal $ax \equiv b \pmod p$.

b) Aplicando la parte a), resolver las congruencias $2x \equiv 1 \pmod{31}$, $6x \equiv 5 \pmod{11}$, y $3x \equiv 17 \pmod{29}$.

10. Suponiendo que a y b son enteros no divisibles por el primo p, establecer lo siguiente:
a) Si $a^p \equiv b^p \pmod{p}$, entonces $a \equiv b \pmod{p}$.
b) Si $a^p \equiv b^p \pmod{p}$, entonces $a^n \equiv b^n \pmod{p^2}$.
[Consejo: Por a), $a = b + pk$ por algún k, de modo que $a^p - b^p = (b + pk)^p - b^p$; ahora demostrar que p^2 divide a la última expresión.]

11. Emplear el Teorema de Fermat para demostrar que, si p es un primo impar, entonces
a) $1^{p-1} + 2^{p-1} + 3^{p-1} + \cdots + (p-1)^{p-1} \equiv -1 \pmod{p}$.
b) $1^p + 2^p + 3^p + \cdots + (p-1)^p \equiv 0 \pmod{p}$.
[Consejo: Recordar que la identidad $1 + 2 + 3 + \cdots + (p-1) = p(p-1)/2$.]

12. Demostrar que si p es un primo impar y k es un entero que satisface $1 \leq k \leq p-1$, entonces la coeficiente binomial

$$\binom{p-1}{k} \equiv (-1)^k \pmod{p}$$

13. Suponer que p y q son primos impares distintos tales que $p - 1 | q - 1$. Si $\text{mcd}(a, pq) = 1$, demostrar que $a^{q-1} \equiv 1 \pmod{pq}$.

14. Si p y q son primos distintos, demostrar que

$$p^{q-1} + q^{p-1} \equiv 1 \pmod{pq}$$

15. Establecer las siguientes afirmaciones:
a) Si el número $M_p = 2^p - 1$ es compuesto, en donde p es un primo, entonces M_p es un seudoprimo.
b) Cada número compuesto $F_n = 2^{2^n} + 1$ es un seudoprimo ($n = 0, 1, 2, \ldots$).
[Consejo: Por el Problema 21 de Sección 2.3, $2^{n+1} | 2^{2^n}$ implica que $2^{2^{n+1}} - 1 | 2^{F_n - 1} - 1$; pero $F_n | 2^{2^{n+1}} - 1$.]

16. Confirmar que los siguientes enteros son seudoprimos absolutos:
a) $1105 = 5 \cdot 13 \cdot 17$
b) $2821 = 7 \cdot 13 \cdot 31$
c) $2465 = 5 \cdot 17 \cdot 29$

17. Demostrar que el seudoprimo más pequeño 341 no es un seudoprimo absoluto demostrando que $11^{341} \not\equiv 11 \pmod{341}$.
[Consejo: $31 \nmid 11^{341} - 11$.]

18. a) Cuando $n = 2p$, en donde p es un primo impar, demostrar que $a^{n-1} \equiv a \pmod{n}$ para cada entero a.
b) Para $n = 195 = 3 \cdot 5 \cdot 13$, verificar que $a^{n-2} \equiv a \pmod{n}$ para cada entero a.

19. Demostrar que cualquier entero de la forma

$$n = (6k + 1)(12k + 1)(18k + 1)$$

es un seudoprimo absoluto si los tres factores son primos; entonces $1729 = 7 \cdot 13 \cdot 19$ es un seudoprimo absoluto.

20. Demostrar que $561|2^{561} - 2$ y $561|3^{561} - 3$. Es una pregunta sin respuesta si existen infinitos números compuestos n con la propiedad que $n|2^n - 2$ y $n|3^n - 3$.

21. Establecer la congruencia

$$2222^{5555} + 5555^{2222} \equiv 0 \pmod{7}$$

[Consejo: primero evaluar 1111 módulo 7.]