TEORÍA ELEMENTAL DE NÚMEROS

DAVID M. BURTON, TRADUCIDO POR PAUL A. LOOMIS

5.3 El Teorema de Wilson

Ahora pasamos a otro hito en el desarrollo de la teoría de números. En su *Meditationes Algebraicae* de 1770, el matemático inglés Edward Waring (1734-1798) anunció varios nuevos teoremas. Principal entre estos es una propiedad interesante de los primos que le informó uno de sus antiguos alumnos, un tal John Wilson. La propiedad es la siguiente: Si p es un número primo, entonces p divide a $(p-1)!+1$. Aparece que Wilson lo ha adivinado sobre la base del cálculo numérico; de todos modos, ni el ni Waring sabían como demostrarlo. Confesando su incapacidad de proporcionar una demostración, Waring anotó, "Los teoremas de este tipo serían muy difícil de demostrar, debido a la ausencia de una notación de expresar los números primos." (Al leer el pasaje, Gauss pronunció su revelador comentario sobre "notaciones versus nociones", implicando que en cuestiones de esta naturaleza lo que realmente importaba era la noción. A pesar del pronóstico pesimista de Waring, poco después Lagrange (1771) dio una demostración de lo que en la literatura se llama "El Teorema de Wilson" y observó que también es válida la reciproca. Tal vez sería más justo nombrar el teorema por Leibniz, como hay evidencia que estaba consciente del resultado casi un siglo antes, pero no publicó nada en el tema.

Ahora damos una demostración del teorema de Wilson.

Teorema 5.4. Wilson. Si p es un primo, entonces $(p-1)! \equiv -1 \pmod{p}$.

Demostracion: Desestimando los casos $p=2$ y $p=3$ por ser evidentes, tomemos $p>3$. Supongamos que a es cualquier de los $p-1$ enteros positivos

$$1, 2, 3, \ldots, p-1$$

y consideramos la congruencia lineal $ax \equiv 1 \pmod{p}$. Entonces $\text{mcd}(a,p)=1$. Por el Teorema 4.7, esta congruencia admite una solución única módulo p; entonces hay un entero único a', con $1 \leq a' \leq p-1$, que satisface $aa' \equiv 1 \pmod{p}$.

Como p es primo, $a=a'$ si y solo si $a=1$ o $a=p-1$. De hecho, la congruencia $a^2 \equiv 1 \pmod{p}$ es equivalente a $(a-1)\cdot(a+1) \equiv 0 \pmod{p}$. Por lo tanto, o $a-1 \equiv 0 \pmod{p}$, en cuyo caso $a=1$, o $a+1 \equiv 0 \pmod{p}$, en cuyo caso $a=p-1$.

Si omitimos los números 1 y $p-1$, el efecto es agrupar los demás enteros $2, 3, \ldots, p-2$ en pares a, a', en donde $a \neq a'$, tales que su producto $aa' \equiv 1 \pmod{p}$. Cuando se multiplican estos $(p-3)/2$ congruencias y se reorganizan los

factores, obtenemos

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

o mejor

$$(p-2)! \equiv 1 \pmod{p}$$

Ahora multiplicamos por $p-1$ para obtener la congruencia

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

como queríamos demostrar.

Ejemplo 5.1. Un ejemplo concreto debería ayudar en clarificar la demostración del teorema de Wilson. Específicamente, tomemos $p = 13$. Es posible dividir los enteros $2, 3, \ldots, 11$ en $(p-3)/2 = 5$ pares, cada producto de cual es congruente a 1 módulo 13. Para escribir estas congruencias explícitamente:

$$\begin{aligned} 2 \cdot 7 &\equiv 1 \pmod{13} \\ 3 \cdot 9 &\equiv 1 \pmod{13} \\ 4 \cdot 10 &\equiv 1 \pmod{13} \\ 5 \cdot 8 &\equiv 1 \pmod{13} \\ 6 \cdot 11 &\equiv 1 \pmod{13} \end{aligned}$$

Multiplicar estas congruencias produce el resultado

$$11! = (2 \cdot 7)(3 \cdot 9)(4 \cdot 10)(5 \cdot 8)(6 \cdot 11) \equiv 1 \pmod{13}$$

y entonces

$$12! \equiv 12 \equiv -1 \pmod{13}$$

Por lo tanto, $(p-1)! \equiv -1 \pmod{p}$, con $p = 13$.

El reciproco del Teorema de Wilson también es verdadero. Si $(n-1)! \equiv -1 \pmod{n}$, entonces n debe ser primo. Porque si n no es primo, entonces n tiene un divisor d con $1 < d < n$. Además, como $d \leq n-1$, d ocurre como uno de los factores en $(n-1)!$, y entonces $d|(n-1)!$. Ahora estamos suponiendo que $n|(n-1)!+1$, y entonces $d|(n-1)!+1$ también. La conclusión es que $d|1$, lo que es una tontería.

Tomado juntos, el Teorema de Wilson y su reciproco proporcionen una condición necesaria y suficiente para determinar primalidad; a saber, un entero $n > 1$ es primo si y solo si $(n-1)! \equiv -1 \pmod{n}$. Desafortunadamente, esta prueba es más de interés teórico que practical como a medida que n aumenta, este rápidamente se vuelve inmanejable en tamaño.

Nos gustaría cerrar este capítulo con una aplicación del Teorema de Wilson al estudio de congruencias cuadráticas. [Se entiende que *congruencia cuadrática* significa una congruencia de la forma $ax^2 + bx + c \equiv 0 \pmod{n}$, con $a \not\equiv 0 \pmod{n}$.] Este es el contenido del Teorema 5.5.

Teorema 5.5. La congruencia cuadrática $x^2 + 1 \equiv 0 \pmod{p}$, en donde p es un primo impar, tiene solución si y solo si $p \equiv 1 \pmod{4}$.

Demostración. Sea a cualquier solución de $x^2 + 1 \equiv 0 \pmod{p}$, de modo que $a^2 \equiv -1 \pmod{p}$. Como $p \nmid a$, el resultado al aplicar el Teorema de Fermat es

$$1 \equiv a^{p-1} \equiv (a^2)^{(p-1)/2} \equiv (-1)^{(p-1)/2} \pmod{p}$$

La posibilidad que $p = 4k + 3$ por algún k no surge. Si así fuera, tendríamos

$$(-1)^{(p-1)/2} = (-1)^{2k+1} = -1$$

por eso, $1 \equiv -1 \pmod{p}$. El resultado neto de esto es que $p|2$, lo cual es evidentemente falso. Por lo tanto, p debe ser de la forma $4k + 1$.

Ahora en la dirección opuesta. En el producto

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

tenemos las congruencias

$$\begin{aligned} p - 1 &\equiv -1 \pmod{p} \\ p - 2 &\equiv -2 \pmod{p} \\ &\vdots \\ \frac{p+1}{2} &\equiv -\frac{p-1}{2} \pmod{p} \end{aligned}$$

Reorganizar los factores produce

$$\begin{aligned} (p-1)! &\equiv 1 \cdot (-1) \cdot 2 \cdot (-2) \cdots \frac{p-1}{2} \cdot \left(-\frac{p-1}{2}\right) \pmod{p} \\ &\equiv (-1)^{(p-1)/2} \left(1 \cdot 2 \cdots \frac{p-1}{2}\right)^2 \pmod{p} \end{aligned}$$

como hay $(p-1)/2$ signos menos involucrados. Es en este punto donde se puede aplicar el Teorema de Wilson; porque, $(p-1)! \equiv -1 \pmod{p}$, de donde

$$-1 \equiv (-1)^{(p-1)/2} \left[\left(\frac{p-1}{2}\right)!\right]^2 \pmod{p}$$

Si asumimos que p es de la forma $4k+1$, entonces $(-1)^{(p-1)/2} = 1$, dejándonos con la congruencia

$$-1 \equiv \left[\left(\frac{p-1}{2}\right)!\right]^2 \pmod{p}$$

La conclusión es que el entero $[(p-1)/2]!$ satisface la congruencia cuadrática $x^2 + 1 \equiv 0 \pmod{p}$.

Echemos un vistazo a un ejemplo real, digamos el caso $p = 13$, lo que es un primo de la forma $4k + 1$. Aquí tenemos $(p - 1)/2 = 6$, y es fácil ver que

$$6! = 720 \equiv 5 \pmod{13}$$

y

$$5^2 + 1 = 26 \equiv 0 \pmod{13}$$

Por lo tanto, la afirmación que $[((p - 1)/2)!]^2 + 1 \equiv 0$ es correcto para $p = 13$.

El Teorema de Wilson implica que existen infinitos números compuestos de la forma $n!+1$. Por otro lado, es una pregunta abierta si $n!+1$ es primo para infinitos valores de n. Los únicos valores en el rango $1 \leq n \leq 100$ para los cuales se sabe que $n!+1$ es un número primo son $n = 1, 2, 3, 11, 27, 37, 41, 73$, y 77. Actualmente, el primo más grande de la forma $n! + 1$ es $6380! + 1$, descubrido en 2000.

PROBLEMAS 5.3

1. a) Hallar el resto cuando se divide 15! por 17.
b) Hallar el resto cuando se divide 2(26!) por 29.

2. Determinar si 17 es un primo decidiendo si $16! \equiv -1 \pmod{17}$.

3. Organizar los enteros $2, 3, 4, \ldots, 21$ en pares a y b que satisfacen $ab \equiv 1 \pmod{23}$.

4. Demostrar que $18! \equiv -1 \pmod{437}$.

5. a) Demostrar que un entero $n > 1$ es primo si y solo si $(n - 2)! \equiv 1 \pmod{n}$.
b) Si n es un entero compuesto, demostrar que $(n - 1)! \equiv 0 \pmod{n}$, excepto cuando $n = 4$.

6. Dado un número primo p, establecer la congruencia

$$(p - 1)! \equiv p - 1 \pmod{1 + 2 + 3 + \cdots + (p - 1)}$$

7. Si p es un número primo, demostrar que para cualquier entero a,

$$p | a^p + (p - 1)!a \qquad \text{y} \qquad p | (p - 1)!a^p + a$$

[Consejo: Por el Teorema de Wilson, $a^p + (p - 1)!a \equiv a^p - a \pmod{p}$.]

8. Hallar dos primos impares $p \leq 13$ para los cuales se cumpla la congruencia $(p - 1)! \equiv -1 \pmod{p^2}$.

9. Usando el Teorema de Wilson, demostrar que para cualquier primo impar p,

$$1^2 \cdot 3^2 \cdot 5^2 \cdots (p - 2)^2 \equiv (-1)^{(p+1)/2} \pmod{p}$$

[Consejo: Como $k \equiv -(p-k) \pmod{p}$, resulta que

$$2 \cdot 4 \cdot 6 \cdots (p-1) \equiv (-1)^{(p-1)/2} 1 \cdot 3 \cdot 5 \cdots (p-2) \pmod{p}.]$$

10. a) Para un primo p de la forma $4k+3$ demostrar que o

$$\left(\frac{p-1}{2}\right)! \equiv 1 \pmod{p} \qquad \text{o} \qquad \left(\frac{p-1}{2}\right)! \equiv -1 \pmod{p}$$

por eso, $[(p-1)/2]!$ satisface la congruencia cuadrática $x^2 \equiv 1 \pmod{p}$.
b) Usar parte a) para demostrar que si $p = 4k+3$ es primo, entonces el producto de todos lo enteros pares menos que p es congruente módulo p a o 1 o -1.

11. Aplicar el Teorema 5.5 para obtener dos soluciones a cada una de las congruencias cuadráticas $x^2 \equiv -1 \pmod{29}$ y $x^2 \equiv -1 \pmod{37}$.

12. Demostrar que si $p = 4k+3$ es primo y $a^2 + b^2 \equiv 0 \pmod{p}$, entonces $a \equiv b \equiv 0 \pmod{p}$.
[Consejo: Si $a \not\equiv 0 \pmod{p}$, entonces existe un entero c tal que $ac \equiv 1 \pmod{p}$; usar este hecho para contradecir el Teorema 5.5.]

13. Proporcionar los detalles que faltan en la siguiente demostración de la irracionalidad de $\sqrt{2}$: Supongamos $\sqrt{2} = a/b$, con $\text{mcd}(a,b) = 1$. Entonces $a^2 = 2b^2$, de modo que $a^2 + b^2 = 3b^2$. Pero $3|(a^2+b^2)$ implica que $3|a$ y $3|b$, lo que es una contradicción.

14. Demostrar que los divisores primos impares del entero n^2+1 son de la forma $4k+1$.
[Consejo: Teorema 5.5.]

15. Verificar que $4(29!) + 5!$ es divisible por 31.

16. Para un primo p y $0 \le k \le p-1$, demostrar que $k!(p-k-1)! \equiv (-1)^{k+1} \pmod{p}$.

17. Si p y q son primos distintos, demostrar que para cualquier entero a,

$$pq | a^{pq} - a^p - a^q + a$$

18. Demostrar que si p y $p+2$ son un par de primos gemelos, entonces

$$4((p-1)!+1) + p \equiv 0 \pmod{p(p+2)})$$