Teoría de números

Hoja de problemas 8

Docente: Gabriel Chicas Reyes, MSc.
Alumno: Kevin López Aquino

Miércoles 13 de noviembre de 2019

I. Ejercicios del libro

Los siguientes son ejercicios propuestos en el capítulo 2, sección 8 de *An Introduction to the Theory of Numbers*, 5ta. edición, de Niven, Zuckerman y Montgomery.

E5. Sea p un primo impar. Demuestre que a pertenece al exponente 2 módulo p si y solo si $a \equiv -1 \pmod{p}$.

- ($\Rightarrow$) Supongamos que a pertenece al exponente 2 módulo p. Entonces

$$a^2 \equiv 1 \pmod{p},$$

de forma que $p \mid (a-1)(a+1)$. Por el lema de Euclides, p divide a $a-1$ o divide a $p+1$. El primer caso no es posible, dado que contradiría la hipótesis que a pertenece al exponente 2. Por tanto,

$$a \equiv -1 \pmod{p}.$$

($\Leftarrow$) Ahora supongamos que $a \equiv -1 \pmod{p}$. Elevando ambos lados al cudrado, notamos que

$$a^2 \equiv 1 \pmod{p}.$$

Puesto que $p \neq 2$, se sigue que $a \not\equiv 1 \pmod{p}$, de forma que a pertenece al exponente 2 módulo p. ■

E15. Demuestre que si a pertenece al exponente h módulo un primo p y h es par, entonces
$$a^{h/2} \equiv -1 \pmod{p}.$$

- Si $a^h \equiv 1 \pmod{p}$, se sigue que

$$p \mid a^h - 1 = (a^{h/2})^2 - 1^2 = (a^{h/2} - 1)(a^{h/2} + 1).$$

Usando el lema de Euclides, p divide a $a^{h/2} - 1$ o a $a^{h/2} + 1$. Notamos que el primer caso no es posible, pues contradiría nuestra hipótesis que a pertenece al exponente h módulo m. Por tanto, p divide a $a^{h/2} + 1$. Luego,

$$a^{h/2} \equiv -1 \pmod{p}. \ \blacksquare$$

E22. Sea g una raíz primitiva módulo p. Demuestre que

$$(p-1)! \equiv \prod_{k=1}^{p-1} g^k \equiv g^{\frac{p(p-1)}{2}} \pmod{p}.$$

Use este hecho para dar otra demostración de la congruencia de Wilson.

- Para cada i tal que $1 \leq i \leq p-1$, existe un k tal que

$$g^k \equiv i \pmod{p},$$

y $1 \leq k \leq p-1$. Luego, podemos decir que

$$\begin{aligned}(p-1)! &= 1 \cdot 2 \cdot \ldots \cdot (p-1) \\ &\equiv g \cdot g^2 \cdot \ldots \cdot g^{p-1} \\ &\equiv g^{1+2+\ldots+(p-1)} \\ &\equiv g^{\frac{p(p-1)}{2}} \pmod{p}. \ \blacksquare\end{aligned}$$

Con el resultado anterior, podemos dar otra demostración del teorema de Wilson, diferente a la demostración basada en la existencia de inversos multiplicativos.

Teorema de Wilson. Para todo primo p, se tiene que $(p-1)! \equiv -1 \pmod{p}$.

Demostración. Si $p = 2$, la proposición se cumple.
Sea p un primo impar. Puesto que p es primo, tenemos garantía de la existencia de al menos una raíz primitiva. Sea g una raíz primitiva. Por el resultado anterior,

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

En lo anterior, usamos el resultado **ejercicio 15** de esta sección, junto con el hecho que g es raíz primitiva y que p es impar. $\square$

II. Orden módulo m

3. Sea $p \equiv 3 \pmod 4$. Demuestre que no existen elementos de orden 4 en $(\mathbb{Z}/p\mathbb{Z})^{\times}$.

• Del hecho que $p \equiv 3 \pmod 4$ deducimos que existe un entero k tal que

$$p = 4k + 3.$$

Argumentamos por contradicción. Supongamos que existe un elemento de orden 4. Entonces, $4 \mid \varphi(p) = p - 1 = 4k + 2$. De esto se sigue que $4 \mid 4k + 2 - 4k = 2$, lo cual es absurdo.
Por tanto, no pueden existir elementos de orden 4 en $(\mathbb{Z}/p\mathbb{Z})^{\times}$. ■

6. Sea m un entero positivo. Suponga que existe un entero a que satisface $\mathrm{ord}_m(a) = m - 1$. Demuestre que m es primo.

• Demostramos que si m es compuesto, no existe un entero a que satisfaga $\mathrm{ord}_m(a) = m - 1$. Notamos que $\varphi(m) = m - 1$ si y solo si m es primo. Además, si m es compuesto,

$$\varphi(m) < m - 1.$$

Luego, el máximo orden posible de un elemento módulo m es $\varphi(m)$, por lo que no puede existir un entero a cuyo orden sea $m - 1$ cuando m es compuesto. ■

7. Suponga que

$$a^r \equiv 1 \pmod m$$
$$a^s \equiv 1 \pmod m.$$

Demuestre que $a^{\mathrm{mcd}(r,s)} \equiv 1 \pmod m$.

• De la hipótesis deducimos que el orden de a módulo m divide tanto a r como a s. Es decir, $\mathrm{ord}_m(a)$ es un divisor común de r y de s. Por tanto, se sigue que $\mathrm{ord}_m(a) \mid \mathrm{mcd}(r, s)$. Ya que $\mathrm{mcd}(r, s)$ es un múltiplo del orden de a módulo m, inferimos que

$$a^{\mathrm{mcd}(r,s)} \equiv 1 \pmod m. \blacksquare$$

8. Sea p primo. Demuestre que si a tiene orden 3 módulo p, entonces

$$1 + a + a^2 \equiv 0 \pmod{p}$$

y $1 + a$ tiene orden 6 módulo p.

• Usando la hipótesis, notamos que

$$a^3 \equiv 1 \pmod{p}.$$

De forma equivalente,

$$a^3 - 1 \equiv (a-1)(a^2 + a + 1) \equiv 0 \pmod{p}.$$

Esto quiere decir que p divide al producto $(a-1)(1+a+a^2)$. Puesto que p es primo, podemos deducir, en virtud del lema de Euclides, que p divide a $a-1$ o que p divide a $1+a+a^2$.
Notamos que si p divide a $a-1$, se sigue que

$$a \equiv 1 \pmod{p}$$

lo que contradiría el hecho que el orden de a módulo p es 3. Por tanto, concluimos que p divide a $1+a+a^2$. Es decir,

$$1 + a + a^2 \equiv 0 \pmod{p}.$$

• Primero demostramos que $(1+a)^6 \equiv 1 \pmod{p}$. Con tal fin, notemos que

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

donde hemos usado el resultado de la parte anterior. Luego,

$$(1+a)^6 \equiv (1+a)^2(1+a)^2(1+a)^2 \equiv a^3 \equiv 1 \pmod{p},$$

porque el orden de a módulo p es 3.

En este punto, el orden de $1+a$ podría ser 6 o algún divisor de 6, a saber, $1, 2$ o 3. Argumentamos por contradicción. Supongamos que el orden de $1+a$ no es 6.

Caso I. Si el orden de $1+a$ es 1, esto implicaría que $a \equiv 0 \pmod{p}$, de forma que a no tendría orden definido, contradiciendo nuestra hipótesis. Por tanto, este caso no es posible.

Caso II. Si el orden de $1+a$ es 2, obtenemos que

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

por la parte anterior. Esto contradiría el hecho que $\operatorname{ord}_p(a) = 3$. Así, este caso tampoco es posible.

Caso III. Ahora supongamos que el orden de $1+a$ es 3. Entonces,

$$\begin{aligned} (1+a)^3 &\equiv 1 \pmod{p} \\ a(1+a) &\equiv 1 \pmod{p} \\ a^2+a &\equiv 1 \pmod{p} \\ a^2+a+1 &\equiv 2 \pmod{p}. \end{aligned}$$

Por la parte anterior, podríamos deducir que $2 \equiv 0 \pmod{p}$, de forma que $p=2$. Pero, en vista que $\operatorname{ord}_p(a)=3$, esto es absurdo. Luego, este caso tampoco es posible.

Puesto que ninguno de los casos anteriores es posible, concluimos que

$$\operatorname{ord}_p(1+a)=6. \quad \blacksquare$$

10. Sea a un entero coprimo con m, cuyo inverso multiplicativo módulo m es b. Demuestre que $\operatorname{ord}_m(a)=\operatorname{ord}_m(b)$.

- Sean $h := \operatorname{ord}_m(a)$ y $\ell := \operatorname{ord}_m(b)$. Entonces,

$$b^h \equiv a^h b^h \equiv (ab)^h \equiv 1 \pmod{m}.$$

De lo que deducimos que $\ell \mid h$. Además,

$$a^\ell \equiv b^\ell a^\ell \equiv (ba)^\ell \equiv 1 \pmod{m},$$

de forma que $h \mid \ell$. Por tanto, $h=\ell$.

Corolario. Si a es una raíz primitiva módulo m, su inverso multiplicativo b también lo es. $\blacksquare$

III. Raíces primitivas

13. Si p es impar y $\operatorname{mcd}(k,p)=1$, demuestre que k^2 no es raíz primitiva módulo p.

• Por contradicción. Supongamos que k^2 es una raíz primitiva módulo p. Entonces, apelando al **ejercicio 15** de la sección I, se sigue que

$$k^{p-1} = \left(k^2\right)^{\frac{p-1}{2}} \equiv -1 \pmod{p},$$

lo cual contradiría el pequeño teorema de Fermat, dado que $p \neq 2$. Por tanto, concluimos que k^2 no puede ser una raíz primitiva módulo p impar. ■

15. Sea p impar. Demuestre que el producto de dos raíces primitivas módulo p nunca es una raíz primitiva módulo p.

• Sean g y h dos raíces primitivas módulo p, no necesariamente distintas. Por el resultado del **ejercicio 15** de la sección I, se sigue que

$$g^{\frac{p-1}{2}} \equiv -1 \pmod{p}$$

$$h^{\frac{p-1}{2}} \equiv -1 \pmod{p},$$

de forma que

$$(gh)^{\frac{p-1}{2}} \equiv g^{\frac{p-1}{2}} h^{\frac{p-1}{2}} \equiv 1 \pmod{p}.$$

Argumentamos por contradicción. Supongamos que gh es una raíz primitiva módulo p. Entonces,

$$(gh)^{\frac{p-1}{2}} \equiv -1 \pmod{p}.$$

Lo anterior implicaría que $-1 \equiv 1 \pmod{p}$, contradiciendo nuestra hipótesis que $p \neq 2$. Por tanto, concluimos que gh no puede ser una raíz primitiva módulo p impar. ■

21 (Generalización del teorema de Wilson). Supongamos que m es $2, 4, p^\alpha$ o $2p^\alpha$, donde p es un primo impar y $\alpha \geq 1$. Sea $S := (\mathbb{Z}/m\mathbb{Z})^\times$. Demuestre que

$$\prod_{x \in S} x \equiv -1 \pmod{m}.$$

• Notamos que para cualquier caso de m existe al menos una raíz primitiva módulo m. Si $m = 2$, la proposición es cierta, dado que $1 \equiv -1 \pmod{2}$. Para los demás casos, tenemos que $\varphi(m)$ es un número par. Si llamamos g a nuestra raíz primitiva módulo m, podemos expresar cualquier elemento x en S como una potencia de g:

$$x \equiv g^k \pmod{m},$$

donde $1 \leq k \leq \varphi(m)$. Luego,

$$\prod_{x \in S} x \equiv g \cdot \ldots \cdot g^{\varphi(m)} \equiv g^{\frac{\varphi(m)(\varphi(m)+1)}{2}} \equiv \left(g^{\frac{\varphi(m)}{2}}\right)^{\varphi(m)+1} \equiv -1 \pmod{m}.$$

En lo anterior, hemos usado el hecho que $g^{\varphi(m)/2} \equiv -1 \pmod{m}$, que es un caso particular de lo que se demuestra en el **ejercicio 15** de la sección I. Esto, combinado con el hecho que $\varphi(m) + 1$ es, en este caso, impar, da el resultado deseado. ■

22. Sea p un primo impar. Demuestre que

$$\prod_{x=1}^{\frac{p-1}{2}} x^2 \equiv (-1)^{\frac{p+1}{2}} \pmod{p}.$$

- Recordamos para i tal que $1 \leq i \leq p-1$, se tiene que

$$-i \equiv p - i \pmod{p}.$$

Así,

$$\begin{aligned}\prod_{x=1}^{\frac{p-1}{2}} x^2 = 1^2 \cdot \ldots \cdot \left(\frac{p-1}{2}\right)^2 &\equiv (-1)(p-1) \cdot \ldots \cdot \left(-\frac{p-1}{2}\right)\left(\frac{p+1}{2}\right) \pmod{p} \\ &\equiv (-1)^{(p-1)/2} \cdot 1 \cdot \ldots \cdot (p-1) \pmod{p}.\end{aligned}$$

Para simplificar el producto anterior, usamos una raíz primitiva g módulo p, de forma que

$$\begin{aligned}(-1)^{(p-1)/2} \cdot 1 \cdot \ldots \cdot (p-1) &\equiv (-1)^{(p-1)/2} \cdot g \cdot \ldots \cdot g^{p-1} \pmod{p} \\ &\equiv (-1)^{(p-1)/2} g^{(p(p-1))/2} \pmod{p} \\ &\equiv (-1)^{(p-1)/2}(-1) \pmod{p} \\ &\equiv (-1)^{(p+1)/2} \pmod{p}. \blacksquare\end{aligned}$$

Corolario. Sea p un primo tal que $p \equiv 1 \pmod{4}$. Entonces, se tiene que

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

Demostración. De la hipótesis deducimos que $\frac{p-1}{2}$ es un número par. Combinando esto con el resultado anterior,

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

$\square$