Ejercicio 1. Segundo parcial 2017

a. Probar que 2 es raíz primitiva módulo 19.

b. Sea p es primo y g una raíz primitiva módulo p. Si m es el orden de g en $U(p^2)$, probar que $p-1 \mid m$.

c. Hallar una raíz primitiva módulo $19^2 = 361$.

d. Probar que si x es un entero impar y p es un primo impar, entonces que $x^m \equiv 1 \pmod{2p^2} \Leftrightarrow x^m \equiv 1 \pmod{p^2}$.

e. Hallar una raíz primitiva módulo 722.

a) $\varphi(19) = 18 = 2 \cdot 3^2$

los divisores primos de $\varphi(19)$ son 2 y 3

2 es raíz primitiva modulo 19 $\Leftrightarrow \begin{cases} 2^{18/3} \not\equiv 1 \pmod{19} \\ 2^{18/2} \not\equiv 1 \pmod{19} \end{cases}$

$\Leftrightarrow \begin{cases} 2^{6} \not\equiv 1 \pmod{19} \\ 2^{9} \not\equiv 1 \pmod{19} \end{cases}$

b) $\overset{19}{\overset{\shortparallel}{p}}$ un primo

$\underset{2}{g}$ raíz primitiva modulo p $\longrightarrow$ $g^{p-1} \equiv 1 \pmod{p}$

el orden de g en $U(p^2)$ es m $\longrightarrow$ $g^m \equiv 1 \pmod{p^2}$

queremos probar que $p-1 \mid m$

si probamos que $g^m \equiv 1 \pmod{p}$

$\Leftrightarrow \bar{g}^m = \bar{1}$ en $U(p)$

$\Leftrightarrow o(\bar{g}) \mid m$

$\Leftrightarrow p-1 \mid m$

el orden de g en $U(p^2)$ es m

$\Rightarrow g^m \equiv 1 \pmod{p^2}$

$\Rightarrow g^m \equiv 1 \pmod p$ porque $p \mid p^2$

$\Rightarrow \bar{g}^m = \bar{1}$ en $U(p)$

$\Rightarrow o(g) \mid m$

$\Rightarrow p-1 \mid m$ ✓

c) Raiz primitiva modulo $19^2 = 361$

$$\varphi(19^2) = 19^2\left(1-\frac{1}{19}\right) = 19^2 \cdot \frac{18}{19} = 19 \cdot 18$$

2 es raiz primitiva modulo 19

2 es raiz primitiva modulo 19^2?

queremos ver si el orden de 2 en $U(19^2)$ es $19 \cdot 18$?

por b) tenemos $18 \mid o_{U(19^2)}(2)$

vamos a probar que 2 es raiz primitiva modulo 19^2

tenemos que ver que el orden de 2 en $U(19^2)$ es $\varphi(19^2) = 19 \cdot 18$

sea m el orden 2 en $U(19^2)$

por la parte b) tenemos que $18 \mid m$

además tenemos $m \mid 19 \cdot 18$

entonces hay dos posibilidades para m:

1. $m = 18$ ← tenemos que descarter esta

2. $m = 19 \cdot 18$

para descarter $m = 18$ hay que probar que $2^{18} \not\equiv 1 \pmod{19^2}$

como $2^{18} \equiv 58 \pmod{19^2}$ tenemos $m \neq 18$

$\Rightarrow$ el orden de 2 es $U(19^2)$ es $19 \cdot 18$

$\Rightarrow$ 2 genera $U(19^2)$

$\Rightarrow$ 2 es raiz primitiva modulo 19^2

d) x entero impar $\rightarrow$ $x \equiv 1 \pmod 2$

p primo impar

queremos probar:

$$x^m \equiv 1 \ (\text{mod } \underbrace{2p^2}_{722}) \iff x^m \equiv 1 \ (\text{mod } \underbrace{p^2}_{361})$$

$$x^m \equiv 1 \pmod{2p^2} \iff \begin{cases} x^m \equiv 1 \pmod 2 \\ x^m \equiv 1 \pmod{p^2} \end{cases}$$

$$\iff \begin{cases} 1^m \equiv 1 \pmod 2 \\ x^m \equiv 1 \pmod{p^2} \end{cases} \quad \text{porque } x \equiv 1 \pmod 2$$

$$\iff x^m \equiv 1 \pmod{p^2}$$

e) Hallar raiz primitiva modulo 722

$722 = 2 \cdot 19^2$

vimos que 2 es raiz primitiva modulo $19^2 = 361$

tomamos $x = 2 + 361 = 363$

veamos que 363 es raiz primitiva modulo 722

$\varphi(722) = \varphi(2 \cdot 19^2) = \varphi(2)\,\varphi(19^2) = \varphi(19^2) = 19 \cdot 18$

tenemos que ver que el orden de 363 en $U(722)$ es $19 \cdot 18$

sea m el orden de 363 en $U(722)$

$$363^m \equiv 1 \pmod{722} \iff 363^m \equiv 1 \pmod{19^2}$$

$\iff$ el orden de 363 en $U(19^2)$ divide a m

$\iff 19 \cdot 18 \mid m$

$$\left.\begin{array}{l} 19\cdot 18 \mid m \\ m \leq 19\cdot 18 \end{array}\right] \Rightarrow m = 19\cdot 18$$

entonces el orden de 363 en $U(722)$ es $19\cdot 18 = \varphi(722)$

$\Rightarrow$ 363 es raiz primitiva modulo 722

Teorema de Lagrange

Resta entonces definir la relación de equivalencia en G que cumpla con lo deseado: para $g, g' \in G$ definimos $g \sim g'$ si existe $h \in H$ tal que $g = hg'$; o equivalentemente, $g \sim g'$ si $g(g')^{-1} \in H$. Veamos primero que esto define una relación de equivalencia:

- (reflexiva) Para todo $g \in G$, tenemos que $g \sim g$ pues $g = eg$ y $e \in H$ (pues H es subgrupo de G.)
- (simétrica) Sean $g, g' \in G$ tales que $g \sim g'$. Entonces $g(g')^{-1} \in H$. Al ser H un subgrupo, es cerrado por inversos y por lo tanto $\left(g(g')^{-1}\right)^{-1} \in H$. Por lo tanto $g'g^{-1} \in H$ y entonces $g' \sim g$.
- (transitiva) Si $g \sim g'$ y $g' \sim g''$ entonces existen $h, h' \in H$ tales que $g = hg'$ y $g' = h'g''$. Por lo tanto tenemos que $g = hg' = h(h'g'') = (hh')g''$. Al ser H un subgrupo (en particular cerrado con la operación) tenemos que $hh' \in H$ y entonces $g \sim g''$.

Resta ver entonces que una clase de equivalencia tiene tantos elementos como H. Observar que si $g' \in G$ entonces la clase de equivalencia de g' es $C = \{g \in G : g \sim g'\} = \{g \in G : \exists h \in H : g = hg'\}$. Por lo tanto $C = \{hg' : h \in H\}$. Además, al multiplicar a todos los elementos de H por g', no hay repeticiones; es decir que si $h_1 \neq h_2$ entonces $h_1 g' \neq h_2 g'$ (por la propiedad cancelativa). Por lo tanto $\#C = |H|$. $\square$

relación de equivalencia:

$g, g' \in G$

$g \sim g'$ si existe $h \in H$ tal que $g = hg' \Leftrightarrow g(g')^{-1} = h$

clase de equivalencia de un elemento $g \in G$:

$$[g] = \{g' \in G : g \sim g'\} = \{g' \in G : g' \sim g\}$$
$$= \{g' \in G : g' = hg \text{ para algún } h \in H\}$$
$$= Hg$$