3. (a) Definir la función de Euler. Enunciar el Teorema de Euler.

(b) Probar que para todo $m, n \in \mathbb{N}$:

$$m, n > 1 \text{ y coprimos } \Rightarrow \varphi(mn) = \varphi(m)\varphi(n)$$

(c) Calcular $\boxed{6397}^{6397}$ módulo 360.

(c) Primero reducimos 6397 módulo 360, obteniendo 277. Como $360 = 2^3 \times 3^2 \times 5$ y 277 no es divisible entre ninguno de los factores 2, 3 y 5, entonces 277 y 360 son coprimos. Por otra parte $\varphi(360) = \varphi(2^3)\varphi(3^2)\varphi(5) = 4 \times 6 \times 4 = 96$, usando la fórmula que se probó en la parte b y que $\varphi(p^k) = p^k - p^{k-1}$ cuando p es primo. Reduciendo el exponente módulo 96 obtenemos 61. Entonces, tenemos que calcular 277^{61} módulo 360.

$61 = 2^5 + 2^4 + 2^3 + 2^2 + 1$ (61 en base 2 es 111101), de modo que

$$277^{61} = 277^{2^5} \times 277^{2^4} \times 277^{2^3} \times 277^{2^2} \times 277$$

(método de exponenciación rápida, visto en el curso).

La siguiente tabla recoge módulo 360 los sucesivos valores de 277^{2^i} con $i = 0, 1, 2, 3, 4$ y 5 (recordar la fórmula recursiva $a^{2^{i+1}} = (a^{2^i})^2$):

i	277^{2^i}
0	277
1	$76729 \equiv_{360} 49$
2	$2401 \equiv_{360} 241$
3	$58081 \equiv_{360} 121$
4	$14641 \equiv_{360} 241$
5	$58081 \equiv_{360} 121$

277^{2^0}

277^2

49^2

Entonces $277^{61} \equiv_{360} 121 \times 241 \times 121 \times 241 \times 277 \equiv_{360} 277$ ya que $121 \times 241 \equiv_{360} 1$.

Una alternativa es plantear que $x \equiv_{360} 6397^{6397}$ si y sólo si:

$$\begin{cases} x \equiv_8 6397^{6397} \\ x \equiv_9 6397^{6397} \\ x \equiv_5 6397^{6397} \end{cases} \Rightarrow \begin{cases} x \equiv_8 5 \\ x \equiv_9 7 \\ x \equiv_5 2 \end{cases}.$$

$\varphi(8) = (2^3 - 2^2) = 4$

$\varphi(9) = (3^2 - 3) = 6$

$\varphi(5) = (5-1) = 4$

Esta reducción se hace aplicando Euler en cada exponente y reduciendo las bases en los respectivos módulos. Aplicando las técnicas vistas en el curso se puede resolver este sistema en congruencias, reduciéndolo a $x \equiv_{360} 277$.

nos piden $a \equiv 6397^{6397} \pmod{360}$ t.q. $0 \leq a < 360$

① $6397^{6397} \equiv 277^{6397}$ (Reduce)

② $\mathrm{mcd}(277, 360) = 1 \Rightarrow$ podemos aplicar Fermat-Euler.

③ $\varphi(360) = \varphi(2^2 3^2 5) = \ldots = 96$.

$277^{\boxed{6397}} \pmod{360}$, sabemos que $277^{\boxed{96}} \equiv 1 \pmod{360}$

$277^{6397} = 277^{96 \cdot k + 61}$

$\equiv (277^{96})^k \cdot 277^{61} \pmod{360}$

$\equiv 277^{61} \pmod{360}$

Queremos hallar $a^e \bmod 360$ $\quad e = 61$

Escribimos 61 en base 2: $61 = 1 + 60$

$= 1 + 2 \cdot (30$

$= 1 + 2 \cdot (2 \cdot 15)$

$= 1 + 2 \cdot (2 \cdot (2 \cdot 7 + 1))$

$= 1 + 2 \cdot (2 \cdot (2 \cdot (2 \cdot 3 + 1) + 1))$

$= 1 + 2 \cdot (2 \cdot (2 \cdot (2 \cdot (2+1) + 1) + 1))$

$= 1 + 2(2 \cdot (2 \cdot (2^2 + 2) + 1) + 1)$

$= 1 + 2(2 \cdot (2^3 + 2^2 + 2) + 1)$

$= 1 + 2 + 2^2 + 2^3 + 2^4 + 2^5$

$= 2^5 + 2^4 + 2^3 + 2^2 + 2^0$

Necesitamos calcular $277^{2^5+2^4+2^3+2^2+2^0}$

$\equiv 277 \cdot 277^4 \cdot 277^{2^3} \cdot 277^{2^4} \cdot 277^{2^5}$

$70^{151} \pmod{252}$

1) $0 < 70 < 252$ ✓

2) $mcd(70,252)=2$. $\rightarrow$ No usamos T. Euler directamente.

$252 = 28 \cdot 9$

$\boxed{= 2^2 \cdot 3^2 \cdot 7}$

$$\begin{cases} x \equiv 70^{151} \pmod{9} \\ x \equiv 70^{151} \pmod{28} \end{cases}$$

$$\begin{cases} x \equiv 70^{151} \ (9) \\ x \equiv 70^{151} \ (7) \\ x \equiv 70^{151} \ (4). \end{cases}$$

Reducimos:

$$\begin{cases} x \equiv 7^{151} \pmod{9} \\ x \equiv 14^{151} \pmod{28} \end{cases}$$

$\varphi(9) = (3^2 - 3) = 6 \rightsquigarrow$ T. Euler $7^6 \equiv 1 \ (9)$

$\Rightarrow 7^{151} \equiv 7^{6 \cdot k + 1} \equiv 7 \ (9)$

$x \equiv 14^{151} \pmod{28}$

Obs: no podemos usar Euler porque $mcd(14,28) = 14 \neq 1$.

$14 \cdot 14 = 14 \cdot 2 \cdot 7 = 28 \cdot 7 \equiv 0 \ (28)$.

$$\begin{cases} x \equiv 7 \ (9) \\ x \equiv 0 \ (28) \end{cases}$$

Ejercicio 2.

(a) Sea $n > 1$, $a \in \mathbb{Z}$ un entero y a_0 el resto de dividir a entre n. Demostrar que para cualquier $m > 1$ se tiene que

$$a^m = a_0^m \pmod{n}.$$

(b) Determinar todos los enteros $a \in \mathbb{Z}$ tales que $a^3 = 4 \pmod 5$.

(c) Determinar todos los enteros $a \in \mathbb{Z}$ tales que $a^3 = 3 \pmod 5$.

$a^3 \equiv 4 \pmod 5$ $\quad$ $a^3 \equiv 4 \equiv -1 \pmod 5$

$\boxed{a \equiv -1 \pmod 5}$

$a = 0 \Rightarrow a^3 \equiv 0 \quad (5)$

$a = 1 \Rightarrow a^3 \equiv 1 \quad (5)$

$\boxed{a = 2 \Rightarrow a^3 \equiv 8 \equiv 3 \quad (5)}$

$a = 3 \Rightarrow a^3 \equiv 27 \equiv 2 \quad (5)$

$\boxed{a = 4 \Rightarrow a^3 \equiv (-1)^3 \equiv -1 \quad (5)}$

a	a^2	a^3
0	0	0
1	1	1
2	4	3
3	4	2
4	1	4

La sol es $a \in \mathbb{Z}$: $a \equiv 2 \ (5) \rightarrow a = 5k + 2$ para $a^3 \equiv 3 \ (5)$

$a \equiv 4 \ (5) \rightarrow a = 5k + 4$ $\quad$ $a^3 \equiv 4 \ (5)$

Ejercicio 3. En este ejercicio conviene tener en cuenta que $119 = 7 \times 17$, $76 = 4 \times 19$ y $57 = 3 \times 19$.

(a) Hallar los inversos de 4 en $\mathbb{Z}_{19}$ y de 3 en $\mathbb{Z}_{119}$.

(b) Resolver el siguiente sistema de congruencias:

$$\begin{cases} 4x = 20 \pmod{76} \\ x = 24 \pmod{57} \\ 3x = 4 \pmod{119} \end{cases}$$

$$\begin{cases} 4x \equiv 20 \ (4) \\ 4x \equiv 20 \ (19) \\ x \equiv 24 \ (3) \\ x \equiv 24 \ (19) \\ 3x \equiv 4 \ (119) \end{cases}$$

(a) Hallar el inverso de 4 (mod 19) $\quad$ $4 \cdot 5 = 20 \equiv 1 \ (19) \Rightarrow 4^{-1} = 5 \pmod{19}$

3 (mod 119) $\quad$ $3 \cdot 40 = 120 \equiv 1 \ (119)$

(b) $\begin{cases} 4x \equiv 20 \ (76) \\ x \equiv 24 \ (57) \\ 3x \equiv 4 \ (119) \end{cases}$

Queremos llevarlo a la forma $\begin{cases} x \equiv a_1 \ (76) \\ x \equiv a_2 \ (57) \\ x \equiv a_3 \ (119) \end{cases}$

Ppd. cancelativa: $c \mid n$ y $ca \equiv cb \ (n) \Rightarrow a \equiv b \ (n/c)$

$$\begin{cases} x \equiv 5 \ (19) \\ x \equiv 24 \ (57) \\ x \equiv 41 \ (119) \end{cases}$$

$x \equiv 5 \ (19)$ → Cancelativa

$x \equiv 24 \ (57)$ → por ahora lo dejamos así

$x \equiv 41 \ (119)$ → inverso de 3 módulo 119

Simplificar / Factorizar

$$\begin{cases} x \equiv 5 \ (19) \equiv 5 \ (19) \\ x \equiv 24 \ (3) \equiv 0 \ (3) \\ \cancel{x \equiv 24 \ (19) \equiv 5 \ (19)} \\ x \equiv 41 \ (7) \equiv -1 \ (7) \\ x \equiv 41 \ (17) \equiv 7 \ (17) \end{cases}$$

Sol. particular.