Exercici 37. Comproveu que 2, 5, 18, 32 són arrels primitives mòdul 37. Comproveu que 2, 5 i 32 ho són mòdul 37^{15}, però que 18 no ho és, i que només 5 ho és mòdul $2{\cdot}37^{15}$

Solució 37. Primer hem de veure que 2, 5, 18 i 32 $\in (\frac{\mathbb{Z}}{37\mathbb{Z}})^*$, la qual cosa és trivial, ja que qualsevol element és invertible en un cos (excepte el zero).
Ara bé, sabem que l'ordre de qualsevol element de $(\frac{\mathbb{Z}}{37\mathbb{Z}})^*$ divideix $\varphi(N)$. Així doncs, l'ordre de qualsevol element de $\frac{\mathbb{Z}}{37\mathbb{Z}}$ divideix $\varphi(37) = 36$.
Si la llista de divisors (i de possibles ordres) és D i volem veure que un $b \in (\frac{\mathbb{Z}}{N\mathbb{Z}})^*$ és arrel primitiva, solament hem d'elevar $b^{d_i}, \forall d_i \in D$ i mirar si dóna 1 en alguna d'aquestes. Si no ho fa, llavors $b^{\varphi(N)} \equiv 1 (modN)$ i satisfarà la condició d'arrel primitiva. Si ho fes, b no seria arrel primitiva.
En el nostre cas particular, si volem veure que 2, 5, 18 i 32 són arrels primitives (mod 37), això vol dir que els hem d'elevar a $D = [2, 3, 4, 6, 9, 12, 18]$:

$$
\begin{array}{rl}
2^2 \equiv 4(mod37) & 5^2 \equiv 25(mod37) \\
2^3 \equiv 8(mod37) & 5^3 \equiv 14(mod37) \\
2^4 \equiv 16(mod37) & 5^4 \equiv 33(mod37) \\
2^6 \equiv 27(mod37) & 5^6 \equiv 11(mod37) \\
2^9 \equiv 31(mod37) & 5^9 \equiv 6(mod37) \\
2^{12} \equiv 26(mod37) & 5^{12} \equiv 10(mod37) \\
2^{18} \equiv 36(mod37) & 5^{18} \equiv -1(mod37) \\
2^{36} \equiv 2^{\varphi(37)} \equiv 1(mod37) & 5^{36} \equiv 5^{\varphi(37)} \equiv 1(mod37) \\
18^2 \equiv 28(mod37) & 32^2 \equiv 25(mod37) \\
18^3 \equiv 23(mod37) & 32^3 \equiv 23(mod37) \\
18^4 \equiv 7(mod37) & 32^4 \equiv 33(mod37) \\
18^6 \equiv 11(mod37) & 32^6 \equiv 11(mod37) \\
18^9 \equiv 31(mod37) & 32^9 \equiv 31(mod37) \\
18^{12} \equiv 10(mod37) & 32^{12} \equiv 10(mod37) \\
18^{18} \equiv -1(mod37) & 32^{18} \equiv -1(mod37) \\
18^{36} \equiv 18^{\varphi(37)} \equiv 1(mod37) & 32^{36} \equiv 532^{\varphi(37)} \equiv 1(mod37)
\end{array}
$$

Així doncs, ja tenim que 2, 5, 18 i 32 són arrels primitives a $(\frac{\mathbb{Z}}{37\mathbb{Z}})^*$.

Teorema per resoldre el següent apartat:
Teorema.- Si g és arrel primitiva $(modp^2), p \neq 2$, aleshores g és una arrel primitiva $modp^k), k \geq 1$.
Demostració: Sabem que $g^{p-1} \not\equiv 1(modp^2)$. Volem veure que $g^{p^{k-2(p-1)}}. \not\equiv 1(moodp^k), \forall k \geq 2$. Amb això ssrà suficient, ja que $\varphi(p^k) = p^{k-1}(p-1)$, així doncs, l'ordre del g serà $\varphi(p^k)$. Fem-ho per inducció sobre k.

(i) Cas inicial $(k = 2)$: $g^{p-1} \not\equiv 1(modp^2)$.

(ii) Hipòtesi d'inducció: $g^{pk-2(p-1)} \not\equiv 1(modp^k)$.
$g^{pk-2(p-1)} = 1 + dp^{k-1}, p \nmid d$, ja que $g^{pk-2(p-1)} \equiv g^{\varphi(p^{k-1})} \equiv 1(modp^{k-1})$.
$g^{pk-1(p-1)} = (1 + dp^{k-1})^p \equiv 1 + dp^k(modp^{k+1}) \equiv 1(modp^{k+1})$.
Així doncs, $\#p^{k+1}g = \varphi(p^{k+1}) = p^k(p-1)$.

Un cop fet això, podem fer l'exercici sobre $\frac{\mathbb{Z}}{37^2\mathbb{Z}}$ que és millor que fer-lo sobre $\frac{\mathbb{Z}}{37^{15}\mathbb{Z}}$. Ja hem demostrat abans com buscar arrels primitives, així que ara usarem el Mathematica per estalviar-nos els càlculs.
PrimitiveRootList[37^2]

[2,5,13,15,17,19,20,22,24,32,35,39,42,50,52,54,55,56,57,59,61,69,...,1367]

Per fer l'últim apartat enunciarem un altre teorema:

Teorema.- Si g és una arrel primitiva a $\frac{\mathbb{Z}}{p^t\mathbb{Z}}, p \neq 2, g$ senar, aleshores g és arrel primitiva a $\frac{\mathbb{Z}}{2p^t\mathbb{Z}}$.

Demostració: Per hipòtesi, $g^{\varphi(p^t)} \equiv 1(mod p^t)$.

$\varphi(2p^t) = \varphi(2)\varphi(p^t) = \varphi(p^t) \Rightarrow$

$$\left.\begin{array}{l} g^{\varphi(2p^t)} \equiv 1(mod p^t) \\ g^{\varphi(2p^t)} \equiv 1(mod 2) \end{array}\right\} \Rightarrow \text{Pel T.X.R} \Rightarrow g^{\varphi(2p^t)} \equiv 1(mod 2p^t) \text{ (i no abans)}$$

Així doncs, ja tenim que solament 5 és arrel primitiva $\frac{\mathbb{Z}}{2\cdot 37^{15}\mathbb{Z}}$