Pràctica 7: PSEUDOPRIMERITAT

1. Esbrina el significat de les funcions lògiques `||`, `&&`, `Not`. Cerca la sintaxi d'un test en el *Mathematica*: `PatternTest`.

2. D'acord amb el petit teorema de Fermat, donat un nombre primer p, se satisfà que $a^{p-1} \equiv 1 \pmod{p}$, per a tot $a \in \mathbb{Z}$ primer amb p.

(a) Comprova aquest teorema per a uns quants nombres primers p.

(b) Comprova que el nombre 1632794693 és compost.

3. Hi ha nombres n compostos per als quals $3^{n-1} \equiv 1 \pmod{n}$. Aquests nombres s'anomenen *pseudoprimers en base* 3.

(a) Programa un test de pseudoprimeritat en base 3.

```
pseudoprimer3Q[n_]:=
    If[!PrimeQ[n]&&PowerMod[3, n - 1, n]==1, True, False]
```

(b) Calcula tots els nombres pseudoprimers en base 3 més petits que 10^k per a $2 \leq k \leq 5$.
`Flatten[Position[Range[m], _?pseudoprimer3Q]]`

4. (a) Defineix el concepte de nombre pseudoprimer en una base b qualsevol i programa un test de pseudoprimeritat en base b.

(b) Calcula tots els nombres pseudoprimers en base 2 més petits que 10^k, per a $2 \leq k \leq 5$.

(c) Calcula els nombres compostos, menors que 20000, que siguin pseudoprimers per a totes tres bases 2, 3 i 5.

Definició. S'anomenen nombres de Carmichael (o, també, pseudoprimers absoluts) els nombres enters, compostos i senars, que són pseudoprimers per a totes les bases.

5. Programa un test per a nombres de Carmichael.

```
carmichaelQ[n_Integer?EvenQ] := False
carmichaelQ[n_Integer?PrimeQ] := False
carmichaelQ[n_Integer?OddQ] := Module[{a = 2},
    While[a < n && (GCD[a, n] != 1 || Mod[a^(n - 1) - 1, n] == 0), a++];
    (a == n)
    ]
```

6. Calcula tots els nombres de Carmichael més petits que 10^n, per a $2 \leq n \leq 5$. Comprova amb exemples que satisfan la congruència del petit teorema de Fermat.

Observació. L'any 1994, W. R. Alford, A. Granville i C. Pomerance demostraren l'existència d'una infinitat de nombres de Carmichael (cf. *Ann. of Math*, **140**(3), 703-722).