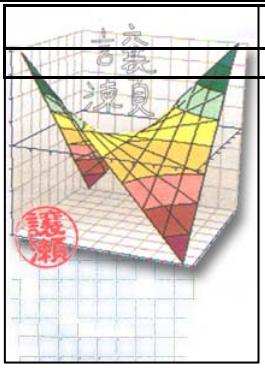

Nom du programme : **SUPERMODULO**
Description : Ce programme permet de calculer le reste de la division euclidienne de a^p par q

On peut écrire également : $a^p \equiv r\,[\text{modulo } q]$ avec $0 \leq r < q$

Remarques :
Ce programme est **indispensable**. Vérifiez qu'il est très difficile (pour les calculatrices CASIO) de trouver le résultat suivant par un autre moyen : $131^{77} \equiv 14\,[\text{mod } 221]$

Le tableur Excel ne pourra pas vous aider non plus, la fonction **mod(131^77 ;221)** retourne une erreur (dépassement de capacité).
Vous comprenez mieux le nom de ce programme …

PROGRAMME

```
"A^P MOD Q, A=":?→A
"P=":?→P
"Q=":?→Q
1→B
1→R
While R<P+1
AxB→B
B – Qx Int(B/Q)→B
R+1→R
WhileEnd
"A^P CONGRU  " :B
```