**Programme MMOD**
Ce programme permet d'effectuer les calculs de congruences.

**Nom du programme :** **MMOD**
**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).

**PROGRAMME (CASIO)**

```
"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
```

**PROGRAMME (TI 89, 92 TI Voyage 200)**

```
mmod()
Prgm
Disp "A^P modulo Q"
Input "Valeur de A : ",a
Input "Valeur de P : ",p
Input "Valeur de Q : ",q
1⟼ b
1⟼ r
While r<p+1
a*b⟼ b
b – q*int(b/q) ⟼ b
r+1 ⟼ r
EndWhile
Disp "A^P est congru à : ",b
EndPrgm
```