

a et n étant deux entiers naturels, l'algorithme détermine si possible le plus petit entier p tel que a^p soit congru à 1 modulo n.

Mathématiques à Valin

http://lycee-valin.fr/maths/exercices_en_ligne/

Code de l'algorithme

```

1  VARIABLES
2  a EST_DU_TYPE NOMBRE
3  n EST_DU_TYPE NOMBRE
4  r EST_DU_TYPE NOMBRE
5  p EST_DU_TYPE NOMBRE
6  b EST_DU_TYPE NOMBRE
7  a2 EST_DU_TYPE NOMBRE
8  DEBUT_ALGORITHME
9  LIRE a
10 LIRE n
11 p PREND_LA_VALEUR 1
12 r PREND_LA_VALEUR a-floor(a/n)*n
13 a2 PREND_LA_VALEUR r
14 TANT_QUE (r!=1 ET p<=n) FAIRE
15   DEBUT_TANT_QUE
16   b PREND_LA_VALEUR r*a2
17   p PREND_LA_VALEUR p+1
18   r PREND_LA_VALEUR b-floor(b/n)*n
19   SI (r==1) ALORS
20     DEBUT_SI
21     AFFICHER a
22     AFFICHER "^"
23     AFFICHER p
24     AFFICHER " est congru à 1 modulo "
25     AFFICHER n
26     FIN_SI
27   FIN_TANT_QUE
28   SI (r!=1) ALORS
29     DEBUT_SI
30     AFFICHER "il n'existe pas d'entier p tel que "
31     AFFICHER a
32     AFFICHER "^p soit congru à 1 modulo "
33     AFFICHER n
34     FIN_SI
35 FIN_ALGORITHME

```

Résultats

```

***Algorithme lancé***
Entrer a : 23
Entrer n : 18
23^6 est congru à 1 modulo 18
***Algorithme terminé***

```