Soit MODEXP = {a, b, c, p | a, b, c, et p sont des entiers binaires positifs tels que $a^b \equiv c \pmod{p}$}

Montrons que MODEXP ∈ P

MODEXP ∈ P s'il existe un algorithme déterministe que le resoud en temps polynomial

1- Trouvons cet algorithme

ALGORITHME : MODEXP

Entrées : a, b, c, p des entiers binaires positifs avec

- a étant la base
- b l'exposant
- c le résultat
- p le modulo

Sorties :

- Vrai si $a^b \equiv c$ [p]
- Faux sinon

Initialisation

résultat = 1

base = a % p

Tant que b > 0 :

Si b est impair, alors :

Résultat = (Résultat * Base) % p

Diviser b par 2 en utilisant un décalage à droite

Base = (Base * Base) % p

Si résultat == c

Retourner Vrai

Sinon

Retourner Faux

2- Vérifions que cet algorithme s’exécute en temps polynomial

La base est mise à jour en utilisant le modulo, ce qui prend O(1).

Boucle principale tant que:

- Vérification si b est positif : O(1).
- Vérification de la parité de b : O(1).
- Mise à jour du résultat (si b est impair) : O(1).
- Division de b par 2 (décalage à droite) : O(1).
- Mise à jour de la base : O(1).

Puisque b est divisé par 2 à chaque itération, le nombre d'itérations de la boucle est O(logb)

Comparaison du résultat final avec c : O(1).

La complexité Totale de notre algorithme est donc

- Initialisation : O(1)
- Boucle : O(logb) itérations × O(1) opérations par itération = O(logb)
- Vérification finale : O(1)

Donc cet algorithme s’exécute en temps O(logb) qui est meilleur que le temps polynomial.

3- Conclusion

Comme MODEXP est soluble par un algorithme déterministe qui s’exécute en temps logarithmique alors MODEXP ∈ P