Nombres pseudo-premiers

Petit théorème de Fermat

Soit a un nombre entier,

si p est premier alors $a^p \equiv a [p]$

Remarque :
Par contraposition, soit a un nombre entier
si $a^n \not\equiv a[n]$ alors n n'est pas premier

Par contre la réciproque n'est pas vraie !

Toutefois, soit a un nombre entier
si $a^n \equiv a[n]$ on considère que n est probablement premier

* Nombres de Poulet

Def : Pour une valeur de a (ou quelques valeurs de a), n vérifie $a^n \equiv a[n]$ et est composé.
n est aussi appelé nombre pseudo-premier de base a.

Le test de primalité de Fermat vérifie pour $a \in \{2;3;5;7\}$ si $a^n \equiv a[n]$: si n vérifie $2^n \equiv 2[n]$ et $3^n \equiv 3[n]$ et $5^n \equiv 5[n]$ et $7^n \equiv 7[n]$
alors on conclut que n est pseudo premiers (relatif)
sinon on conclut que n n'est pas premier.

Problème : quelques nombres sont composés et sont considérés comme pseudo premiers : les nombres de Poulet

Par exemple 341 vérifie $2^{341} \equiv 2[341]$ mais $341 = 11 \times 31$
341 est donc un nombre de Poulet. Mais $3^{341} \not\equiv 3[341]$ donc il n'est pas premier.
C'est pourquoi le test de Fermat effectue le test avec quelques valeurs de a.

---

* Nombres de Carmichael

Def : Pour toutes valeurs de a comprise entre 2 et $n-1$, n vérifie $a^n \equiv a[n]$ et est composé.
n est aussi appelé nombre pseudo premier absolu.

Par exemple : $561 = 3 \times 11 \times 17$
$1105 = 5 \times 13 \times 17$

Test de primalité

- Test de Fermat (nombres de Poulet)

```
Test(p):={
  local a,t;
  t:=0;
  a:=2;
  si irem(a^(p),p)==a   alors
    t:=t+1;
  fsi;

  a:=3;
  si irem(a^(p),p)==a   alors
    t:=t+1;
  fsi;

  a:=5;
  si irem(a^(p),p)==a   alors
    t:=t+1;
  fsi;

  a:=7;
  si irem(a^(p),p)==a   alors
    t:=t+1;
  fsi;

  si t==4 alors
    afficher p+" est probablement un nombre premier";
  sinon
    afficher p+" n'est pas un nombre premier";
  fsi;
}
```

- Test (nombres de Carmichael)

```
Pseudo(p):={
  local a,t;
  t:=0;
  pour a de 2 jusque p-1 faire
    si irem(a^p,p)==irem(a,p) alors
      t:=t+1;
    fsi;
  fpour;
  si t==p-2 alors
    afficher p+" est un nombre premier ou pseudopremier absolu";
  sinon
    afficher p+" n'est pas un nombre premier";
  fsi;
}
```