Nombre de Fermat

5 décembre 2013

Résumé

L'objectif de ce sujet de travaux-pratiques est d'implanter le test de pseudoprimalité de Fermat pour deviner le caractère premier ou composé des premiers nombres de Fermat !

On représente des nombres par des tableaux de chiffres binaires, les calcul faits sur des registres de taille définie à l'exécution.

```
typedef unsigned char chiffre;
typedef chiffre * nombre;
unsigned int      taille;
void init( uint t );
```

On pourra par exemple manipuler un module global :

```
nombre  module;
void bit( uint i  );
```

Vous pouvez utiliser le fichier de définition modular.h.

```
wget langevin.univ-tln.fr/cours/PAA/tps/fermat/modular.h
```

1 Arithmétique

Implanter la multiplication modulaire des entiers binaires en utilisant la méthode d'addition-duplication.

```
void mult( nombre y, nombre x ); // y := (x * y) % module
```

2 Vérification

Vérifier le bon fonctionnement en utilisant le théorème de Wilson qui affirme que p est premier si et seulement si :

$$(p-1)! \equiv -1 \pmod{p}$$

3 Application

Implanter le test de pseudoprimalité de Fermat, pour l'appliquer à la suite des nombres de Fermat $F_n = 2^{2^n} + 1$ pour $n = 1, 2, 3$, etc...

```
TEST de FERMAT ( m )
    x := residu aleatoire
    n := m - 1
    y := x ^ n  modulo  m
    retourner y == 1
```

On considère un nombre Fermat-premier quand il passe 50 fois le test ci-dessus. Pour cet exercice, vu la forme des nombres de Fermat, il n'est pas nécessaire d'implanter une exponentiation modulaire !

4 Temps de cacul

Donner une formule du temps de calcul pour réaliser un test sur le n-ième nombre de Fermat. Estimer le temps de calcul pour tester F_{33}.

5 Multiprécision

Faire un travail analogue avec la calculette `bc`, puis la bibiliothèque `gmp`.