Examen, 2 heures
Une feuille A4 manuscrite acceptée.

## Exercice 1

On rappelle qu'un nombre $c$ est de Carmichael s'il n'est pas premier et si pour tout $a$ premier avec $c$, on a $a^{c-1} \equiv 1\ [mod\ c]$.

**Question 1** Montrer que si $c$ est sans facteur carré, non-premier, et tel que tout diviseur premier $p$ de $c$ est tel que $p-1$ divise $c-1$, alors c'est un nombre de Carmichael. *Cette question pourra être admise dans la suite.*

**Question 2** Montrer que si $(6t+1)$, $(12t+1)$ et $(18t+1)$ sont premiers, alors leur produit est de Carmichael.

**Question 3** A propos du texte joint [1], ecrit sur SageMath, expliquer ce que fait la fonction UNE FONCTION (en particulier, expliquer ce que l'on peut déduire du résultat retourné, et donner le nom d'un protocole connu s'y rapportant). Critiquer éventuellement.

**Question 4** Que produit la boucle suivante ("In [2]") ?

**Question 5** À quoi doit on s'attendre pour les résultats de "In [3]" et "In [4]" ?

In [1]:
```
def UNE_FONCTION(x):
    C=True
    R=Integers(x)
    for j in range (1,100):
        a=R.random_element()
        if a^((x-1)/2) != jacobi_symbol(a,x):
            C=False
    return C
```

In [2]:
```
for t in range (1000, 1100):
    x1=(6*t+1)
    x2=(12*t+1)
    x3=(18*t+1)
    if UNE_FONCTION(x1)==True:
        if UNE_FONCTION(x2)==True:
            if UNE_FONCTION(x3)==True:
                print x1*x2*x3
```

```
1396066334401
1544001719761
```

In [3]:
```
for a in range (1,400000):
    if gcd(a,1396066334401)==1:
        if mod(a,1396066334401)^(1396066334400) !=1:
            print a
print 'fini'
```

...

In [4]:
```
is_prime(1396066334401)
```

1. != signifie $\neq$

**Exercice 2**

On considère le protocole suivant.

*Alice choisit en secret deux grands nombres premiers* $p, q$.
*Alice calcule en secret* $N = p \times q$.
*Alice choisit en secret un élément aléatoire* $b \in (\mathbb{Z}/N\mathbb{Z})^*$.
*Alice publie* $(N, b)$.
*Bob compose un message* $m \in (\mathbb{Z}/N\mathbb{Z})^*$. *En secret, il calcule* $c = m \times (m + b)$ *modulo* $N$.
*Bob publie* $c$.
*Alice souhaite déchiffrer le message.*

**Question 0** : Alice utilise un protocole inconnu pour choisir ses nombres premiers. Prise d'un doute, elle souhaite vérifier qu'ils sont premiers. Doit-elle utiliser le test de Fermat ou de Solovay-Strassen (et pourquoi) ?

**Question 1-a** : comment Alice peut elle simplement tester si un élément aléatoire de $\mathbb{Z}/N\mathbb{Z}$ est bien dans $(\mathbb{Z}/N\mathbb{Z})^*$ ? (c'est à dire est bien inversible modulo $N$)

**Question 1-b** : combien d'éléments de $\mathbb{Z}/N\mathbb{Z}$ sont ils inversibles modulo $N$ ?

**Question 2-a** : De quelle équation quadratique [2] publique l'élément $m$ est-il solution ?

**Question 2-b** : combien de solutions une telle équation quadratique peut elle avoir dans $\mathbb{Z}/N\mathbb{Z}$ ?

**Question 2-c** : Si $p$ et $q$ sont choisis congrus à 3 modulo 4, Alice retrouve-t-elle facilement les solutions de l'équation de la question 2 ? (et pourquoi ?)

**Question 3** : Expliquer comment, si l'on connait toutes les racines carrées differentes d'un élément $\Delta = \alpha^2 \in \mathbb{Z}/(N\mathbb{Z})$, on peut alors factoriser $N$.

**Question 4** : On suppose que Eve, une espionne, a la possibilité de soumettre plusieurs valeurs de $c$ de son choix au système, et de recevoir des valeurs de $m$ correspondantes (à chaque fois aléatoires parmi les solutions possibles). En utilisant la question précédente, expliquer comment Eve peut ainsi obtenir la factorisation de $N$ (et ainsi briser le protocole). *C'est le chosen-ciphertext-attack.*

Le protocole ici présenté est le systeme de Rabin.

2. de la forme $\alpha X^2 + \beta X + \gamma = 0$