

Nous recommençons avec l'initialisation :

```
pgcde = xgcd
```

et reprenons les exercices du TD.

1. Soit $p = 100003$, $q = 102001$ et $e = 65$.

a. Trouvez u et v tel que $1 = ue + v(p-1)(q-1)$, et alors $e^{-1} \bmod (p-1)(q-1)$:

```
e = 257
p, q = (100003, 102001)
r, u, v = pgcde(e, (p-1)*(q-1))
```

Quel est le valeur de d tel que $ed \bmod (p-1)(q-1) = 1$?

b. Trouvez d_1 et d_2 tel que $d_1 = e^{-1} \bmod (p-1)$ et $d_2 = e^{-1} \bmod (q-1)$.

c. Vérifiez que $d_1 = d \bmod (p-1)$ et $d_2 = d \bmod (q-1)$.

d. Vérifiez pour chaque k dans $0 \leq k \leq 5$, que $d' = k \frac{(p-1)(q-1)}{6}$, aussi satisfait

$$d_1 = d' \bmod (p-1) \text{ et } d_2 = d' \bmod (q-1).$$

2. Pour les mêmes valeurs de p , q et e dans l'exercice précédent, soit $n = pq$ et prenez le message $m = 100$. Pour $up + vq = 1$, rappelez que $\iota(x_1, x_2) = x_1 + (x_2 - x_1)up$ est l'inverse de $\pi(x) = (x_1, x_2) = (x \bmod p, x \bmod q)$.

L'arithmétique modulaire se peut calculer avec les entiers :

```
n, e = (p*q, 257)
m = 100
c = power_mod(m, e, n)
```

ou avec la construction explicite de $\mathbb{Z}/n\mathbb{Z}$:

```
R = IntegerModRing(n)
m = R(100)
c = m^e
```

a. Trouvez $c = m^e \bmod n$, $c_1 = m^e \bmod p$ et $c_2 = m^e \bmod q$ et vérifiez que $c = \iota(c_1, c_2)$.

b. Trouvez $s = m^d \bmod n$, $s_1 = m^{d_1} \bmod p$ et $s_2 = m^{d_2} \bmod q$ et vérifiez que $s = \iota(s_1, s_2)$.

- c. Vérifiez que s est la signature de m .
 - d. Quels sont les étapes audessus qui peuvent être fait avec la clé RSA publique et quels ont besoin de la clé privée?
3. Soit $p = 100000000003$, $a = 2$, et $b = 3$.
- a. Trouvez k tel que $b = a^k \pmod p$. Alors k est la clé privée associée à la clé publique ElGamal (p, a, b) .
 - b. Calculez un chiffrement c de $m = 7$ avec (p, a, b) .
 - c. Montrez les étapes pour déchiffrement de votre texte chiffré.