Opérations à implémenter
addition grand nombre
soustraction grand nombre
multiplication grand nombre => 12

addition/soustraction modulaire = >14

Multiplication de Montgomery
passage à la représentation de Montgomery => 16

RSA complet partie chiffrement et déchiffrement => 20 /20

Addition Modulaire
I+J mod N =

I<N
J< N

si I+J>N : I+J-N   sinon I+J

Multiplication Modulaire

A et B sont écrits dans la représentation de Montgomery

Soit N, le modulo de taille 1024 en bits, R est la plus petit puissance de 2 supérieure à N : soit le min de l'ensemble... 2^1025
Alors V est défini comme l'opposé de l'inverse de N mod R
RxR' + Nx(-V) = 1

bonus : R^2 mod N

au+bv = pgcd(a,b) (1 quand a est b sont premiers entre eux)
au + bv mod b = au =

au = 1 mod b

L'alorithme ci-dessous correspond à la multiplication de Montgomery des entrées I et J

Algorithme MultMtg
1) S = IxJ (multiplication normale dite school book)
2) T = Sx$\underline{V}$ mod $\underline{R}$ (nombre de taille inférieur à celle de R)
3) M = S+Tx$\underline{N}$
4) U = M/R
5) si U>N : U-N   sinon U

Mode brouillon activé :

RxR' + Nx(-V) = 1

modulo R on obtient : $N(-V) = 1 \bmod R$

$N = -1/V \bmod R$

$T = S \times (-1/N) \bmod R$

$M = S + [S \times (-1/N) \times N \bmod R]$

$M = S + [-S \bmod R]$ avec $S = S_1 \times R + S_0$
$M = S_1 \times R + S_0 + [-S_0]$
$M = S_1 \times R$
$U = M/R = S_1$ partie haute de $A \times B$

conséquence : $0 < U < 2N$

Question en suspens : comment trouver la représentation de Montgomery de A et B ?
Représentation classique Mtg

A	phi(A)
B	phi(B)

$\mathrm{phi}(A) = A \times R \bmod N$
$\mathrm{phi}(B) = B \times R \bmod N$

$\mathrm{MultMtg}(I,J) = I \times J \times R^{-1} \bmod N$

$\mathrm{phi}(A) = \mathrm{MultMtg}(A, R^2 \bmod N)$

$A \times R^2 \times R^{-1} = A \times R \bmod N$

Réciproquement
$A = \mathrm{MultMtg}(\mathrm{phi}(A),1) = \mathrm{phi}(A) \times R^{-1} \bmod N = a \times R \times R^{-1} \bmod N$