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
$R \times R' + N \times (-V) = 1$

$au+bv = \mathrm{pgcd}(a,b)$ (1 quand a est b sont premiers entre eux)
$au + bv \bmod b = au =$

$au = 1 \bmod b$

1) $S = A \times B$ (multiplication normale dite school book)
2) $T = S \times V \bmod R$ (nombre de taille inférieur à celle de R)
3) $M = S+T \times N$
4) $U = M/R$
5) si $U>N$: $U-N$ sinon U

Mode brouillon activé :

$R \times R' + N \times (-V) = 1$

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)

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

$MultMtg(I,J) = IxJxR\{-1\} \bmod N$

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

$AxR^2xR^{-1} = AxR \bmod N$

Réciproquement
$A = MultMtg(phi(A),1) = phi(A)xR^{-1} \bmod N = axRxR^{-1} \bmod N$