

Начало

isEven(N) || N[0]%5==0 ?

да

Возврат multiplyRingDirect(x,y,N)

Конец

нет

BigInt R(4), Ns(4), w(4)

createMontgomery(N, R, Ns, w)

Возврат
multiplyRingMontgomery
(x, y, N, R, Ns, w)

Конец

