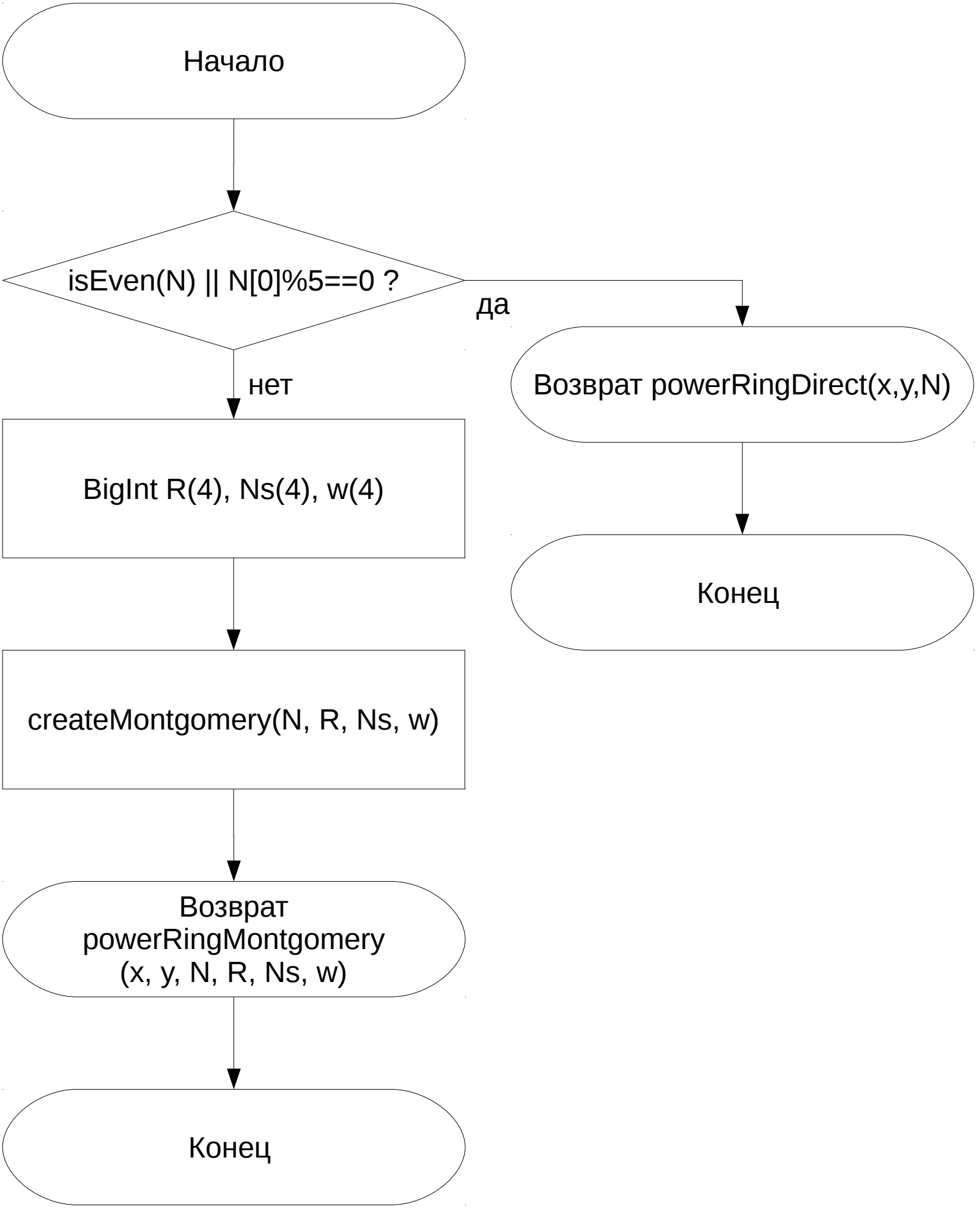
Начало
isEven(N) || N[0]%5==0 ?
да
нет
Возврат powerRingDirect(x,y,N)
Конец
BigInt R(4), Ns(4), w(4)
createMontgomery(N, R, Ns, w)
Возврат
powerRingMontgomery
(x, y, N, R, Ns, w)
Конец