Начало

BigInt rev(x.m_nExp)

BigInt divisor =
gcd(x, modulo, &rev)
/* Вычислить НОД и 1-й коэфф.
линейного представления */

|divisor| == 1 ?

да

Возврат 0

Конец

нет

BigInt remainder(x.m_nExp)

divide(rev, modulo, &remainder)

rev < 0 ?

да

remainder = subtractNaive
(modulo, remainder)

нет

Возврат remainder

Конец