АНАЛИЗ НА РЕШЕНИЕТО НА ЗАДАЧА
ОБРАТНИ ЧИСЛА

Наивната идея за решаване на уранението ($a.b$) $mod\ m = 1$ е да се направи един цикъл за b=0, 1, 2, ..., m-1 и за всяка стойност на b да се проверява дали остатъкът при деление на произведението ($a.b$) с m е равен на 1. Това решение ще получи 50 точки, защото за големи стойности на m се бави твърде много. Програмната реализация е показана в inverse_naive.cpp.

За 100 точки трябва да се използва разширения алгоритъм на Евклид за намиране на x и y, такива че $a.x + m.y = d$, където d=НОД(a, m). Но по условие m е просто число и $1 \leq a < m$, така че d=1, т.е. $a.x + m.y = 1$. Коефициентът на Безу x се явява решение на уравнението $(a.b)\ mod\ m = 1$. Тази идея е реазлизирана в inverse.cpp.

Автор: Кинка Кирилова-Лупанова