34 Умножение и обращение

Задача. Умножение по простому модулю $p = 2^{256} - 189$, используемому в СТБ 34.101.45, выполняется за 1 мкс, а мультипликативное обращение по этому модулю — за 100 мкс. Бобу требуется написать программу, которая обрабатывает переменные $X_i, Y_i \in \{1, 2, \ldots, p - 1\}$ и на месте X_i возвращает $X_i * Y_i^{-1} \bmod p$, $i = 1, 2, \ldots, 100$. Вычисления должны быть выполнены не более чем за 500 мкс. Дополнительные переменные вводить нельзя. Помогите Бобу.

Решение. Искомый (при $n = 100$) алгоритм имеет следующий вид:

1. Для $i = 2, \ldots, n$:
   (a) $X_i \leftarrow X_i * Y_1 \bmod p$;
   (b) $Y_1 \leftarrow Y_1 * Y_i \bmod p$;
2. $Y_1 \leftarrow Y_1^{-1} \bmod p$.
3. Для $i = n, \ldots, 2$:
   (a) $X_i \leftarrow X_i * Y_1 \bmod p$;
   (b) $Y_1 \leftarrow Y_1 * Y_i \bmod p$;
4. $X_1 \leftarrow X_1 * Y_1 \bmod p$.

Сложность алгоритма: 1 обращение и $4n - 3$ умножений. При $n = 100$ алгоритм выполняется за 497 мкс.

Алгоритм соответствует известному методу П. Монтгомери одновременного обращения нескольких чисел по одному модулю. Единственным отличием является организация вычислений таким образом, чтобы можно было обойтись без дополнительных переменнных. □