38 Комбинаторный компьютер

Задача. Трент научился управлять большими ансамблями квантовых частиц и построил компьютер, который может эффективно решать различные комбинаторные задачи, например, за приемлемое время вычислять значение функции

$$f(n, m, k) = |\{\text{всевозможные сочетания из } m \text{ по } k \text{ частиц}\}| \bmod n.$$

Покажите, как с помощью компьютера Трента Боб может за приемлемое время разложить на множители большое составное число.

Решение. Пусть n — число, которое требуется факторизовать, и пусть

$$g(n, m) = \begin{cases} 1, & \gcd(m! \bmod n, n) > 1, \\ 0, & \text{в противном случае.} \end{cases}$$

Если p – минимальное натуральное, для которого $g(n, p) = 1$, то p — минимальный делитель n. Если Боб располагает эффективным алгоритмом вычисления $g(m, n)$, то дихотомией отрезка $\{2, 3, \ldots, [\sqrt{n}]\}$ он может эффективно находить p с последующей факторизацией n.

Для вычисления $g(n, m)$ Боб может использовать следующий рекурсивный алгоритм:

1. Если $m = 1$, то возвратить 1.
2. Выбрать $k = [m/2]$ и вычислить $g(n, k)$.
3. Если $g(n, k) = 1$, то возвратить 1:
$$\gcd(m! \bmod n, n) \geq \gcd(k! \bmod n, n) > 1.$$
4. Обратиться к компьютеру Трента и вычислить
$$f(n, m, k) = \frac{m(m-1)\ldots(m-k+1)}{k!} \bmod n.$$
Поскольку $g(n, k) = 0$, $g(n, m) = 1$ тогда и только тогда, когда $\gcd(f(n, m, k), n) > 1$.
5. Возвратить 1, если $\gcd(f(n, m, k), n) > 1$, и 0 в противном случае.

□