МФТИ
Алгоритмы и структуры данных, осень 2022
Семинар №07. Теория чисел

1. По данным числам a, b найдите целые x, y, такие что $ax + by = (a, b)$. Для каждого c опишите все решения уравнения $ax + by = c$.
2. За $O(n)$ для каждого $i \in [2, n]$ найдите $mind(i)$ — минимальный простой делитель i.
3. Дано простое число p, а также число a, причём $(a, p) = 1$. Как найти $a^{-1} \pmod p$?
4. Дано произвольное число m, а также число a, причём $(a, m) = 1$. Как найти $a^{-1} \pmod m$?
5. Приведите эффективный алгоритм для вычисления $a^{b^c} \pmod p$ для целых положительных a, b, c и простого p.
6. Найдите наибольший общий делитель двух **длинных** чисел a и b за полиномиальное время от их длины.
7. Найдите обратные к $1, 2, \ldots, n$ по простому модулю p за $O(n)$.
8. Найдите
а) $\sum\limits_{k=0}^{n} C_n^k$;
б) $\sum\limits_{k=0}^{n} k \cdot C_n^k$;
в) $\sum\limits_{k=0}^{n} k^2 \cdot C_n^k$.
9. Пусть дано n чисел от 2 до L. Проверьте каждое из них на простоту на общее время $O(\sqrt{L} + n\sqrt{L}/\log L)$.
10. Найдите количество пар целых положительных чисел (x, y), таких что $xy \leqslant n$, за $O(\sqrt{n})$.
11. За $O(\sqrt{n})$ найдите количество целых чисел в отрезке $[1, n]$, свободных от квадратов.
12. Найдите $\Phi(n) = \sum\limits_{k=1}^{n} \varphi(k)$, где $\varphi(\cdot)$ — функция Эйлера. Это число равно количеству пар взаимно простых чисел (a, b) с условиями $1 \leqslant a \leqslant b \leqslant n$. Асимптотика: а) $O(n)$; б) $O(n^{3/4})$.
13. Пусть g — первообразный корень по простому модулю p, то есть $\{g^0, g^1, \ldots, g^{p-2}\} = \{1, 2, \ldots, p-1\} \pmod p$. Предложите способ решать уравнения вида $g^x = a \pmod p$ за $O(\sqrt{p})$ в среднем.