

Задание 5. Битовые операции, модульная арифметика, немного рекуррент.

- 1 Оцените сложность алгоритма Divide, приведенного на странице 19 книги Дасгупты.
- 2 Предложите алгоритм возведения n -битовых чисел в n -битовую степень по n -битовому модулю, оцените его сложность.
- 3 Кто-то очень умный пришел и сказал, что умеет возводить числа из n бит в квадрат за линейное время. Докажите, что тогда можно перемножать и разные числа за O от максимума их длин.
- 4 Докажите, что $\text{НОД}(a, b) = \text{НОД}(a - b, b)$.
- 5 На доске написан набор положительных целых чисел. За один ход можно взять любые два числа и вычесть из большего меньшее. Процесс останавливается, когда все числа становятся одинаковыми. Докажите, что этот процесс всегда остановится. Какие числа останутся в результате?
- 6 Оцените асимптотику рекурренты $T(n) = T(\alpha n) + T((1 - \alpha)n) + \Theta(n)$ для $\alpha \in (0, 1)$.
- 7 Оцените трудоемкость алгоритма, разбивающего задачу размера n на n подзадач размера $\frac{n}{2}$, используя для этого $\Theta(n)$ операций.