# Задача

Доказать, что задача «Составные числа»$\in NP$.

## Постановка

Задано натуральное число $n$. Составное ли оно, т.е. имеет ли ононатуральный неединичный и не равный $n$ делитель?

Решение

## Генерация подсказки

В качестве подсказки для машины Тьюринга будем использовать всевозможные натуральные числа. Тогда генерация подсказки для каждой следующей машины Тьюринга будет заключаться в прибавлении единицы к предыдущей подсказке, то есть иметь сложность $O(k)$, где $k$— длина подсказки. В случае поставленной задачи только на числах $k < m$ (где m – длина входа) может останавливаться ДМТ с положительным ответом.
Таким образом сложность генерации подсказки: $O(m).$

## Деление уголком

В дальнейшем нам понадобится следующая Лемма:

### Лемма (сложность деления уголком)

Временная сложность нахождения остатка (деления уголком): $T\left(m\right)=O(m^{2})$.

#### Доказательство леммы

Зададим делимое и делитель в двоичной системе.

* Делимое: $x=x\_{m-1} 2^{m-1}+x\_{m-2}2^{m-2}+…+x\_{1}2^{1}+x\_{0}2^{0}$
* Делитель: $y=y\_{k-1}2^{k-1}+y\_{k-2}2^{k-2}+…+y\_{1}2^{1}+y\_{0}2^{0}$

Если $m<k$, то остаток равен $x$, частное —$0$.

Иначе, то есть при $m\geq k$, число шагов при делении уголком двух чисел, записанных в двоичной системе счисления, будет в точности $m-k$. На каждом шаге число битовых операций вычитания будет ограничено $k+1$, т.к. мы работаем с числами, представленными в двоичной системе. Таким образом, общее число битовых операций ограничено сверху $(m-1-k)(k+1)$.

Тогда число битовых операций не превосходит $m^{2}$, и для них выполнена оценка $O\left(m^{2}\right)$.

*Доказательство завершено.*

Если подсказка является делителем числа, то ДМТ, обрабатывающая данную подсказку, дает положительный ответ, в противном случае ДМТ не останавливается.

Для оценки итоговой временной сложности нам необходимо будет выбрать максимальное время работы на ДМТ, давших положительных ответ. (Здесь под работой ДМТ понимается время на генерацию подсказки + время работы самого алгоритма).

Воспользуемся результатом рассуждений, приведенных выше. Генерация подсказки имеет сложность $O(m)$ , алгоритм нахождения остатка имеет временную сложность $O\left(m^{2}\right)$, где $m$— длина входных данных (числа $n$). Итоговая сложность ($O\left(m^{2}\right)$) ограничена полиномом от входных данных. Поэтому задача проверки, является ли число составным, принадлежит классу NP.