

Как правильно раскладывать на множители (докуда проверять)

Разница факторизации и теста на простоту

В 2002 году было доказано, что задача проверки на простоту в общем виде полиномиально разрешима, но предложенный детерминированный тест Агравала — Каяла — Саксены имеет довольно большую вычислительную сложность, что затрудняет его практическое применение.

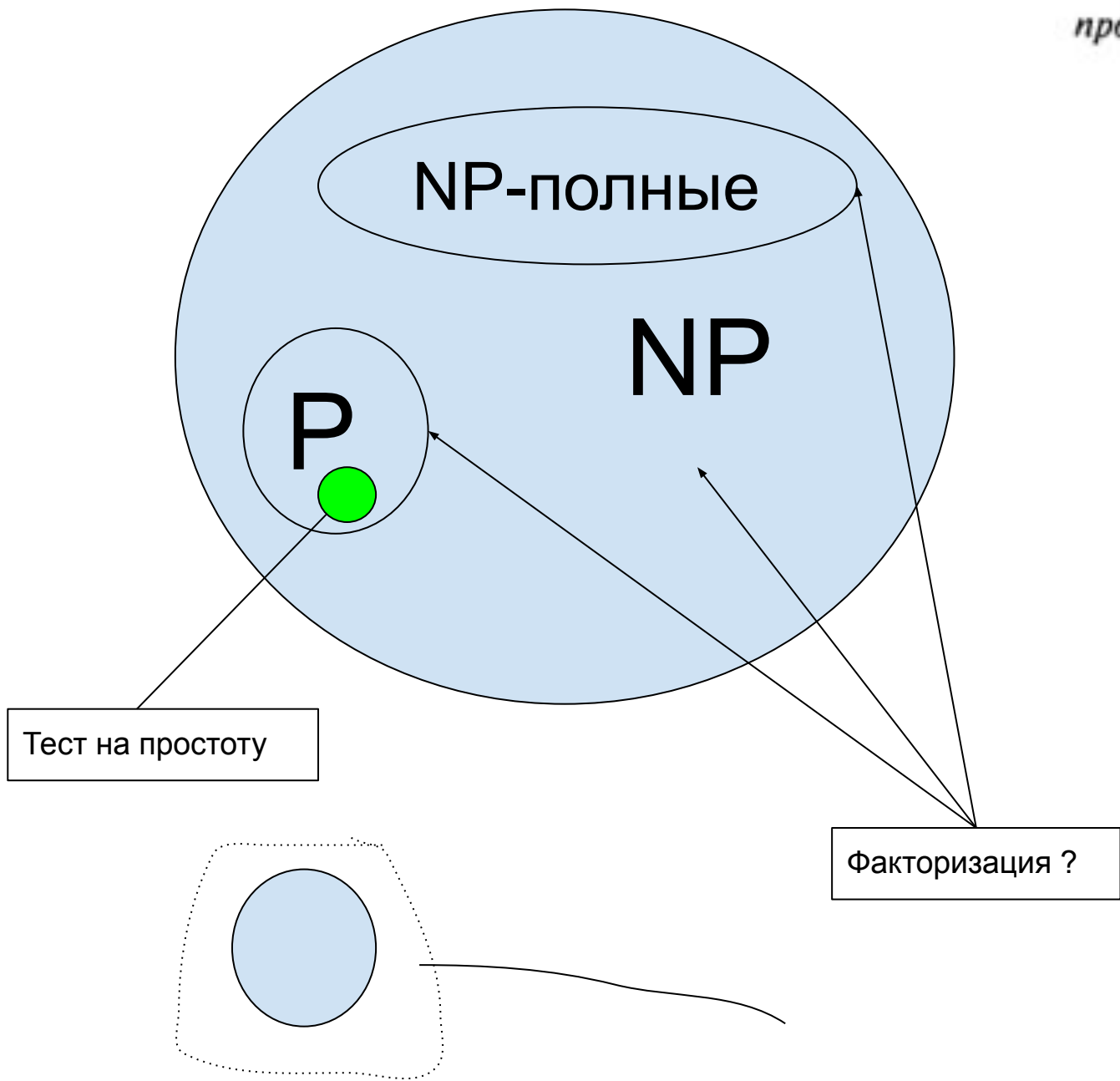
P=?=NP

NP - полные (ряд задач, которые трудноразрешимы, но решение одной решает остальные)

Леня Левин 1970-ые СССР

Есть ли в графе клика (полный подграф с числом вершин не менее k)
есть ли в графе гамильтонов цикл

Квантовые компьютеры
Алгоритм гровера



Полиномиальные алгоритмы
 $n=10001$
 $n^7=10000^7=10^{28}$

Экспоненциальные алгоритмы (равносилен полному перебору)
 2^n
 $2^{10000}=(2^{10})^{1000}=(10^3)^{1000}=10^{3000}$



P!=NP ?
Теория алгоритмов
Теория автоматов

1) Даны n городов и расстояния r_{ij} между ними. Требуется найти циклический маршрут минимальной длины, заходящий во все города по одному разу. Это классический оптимизационный вариант задачи коммивояжера. Вариант «распознавания»: существует ли маршрут, проходящий через все города, длина которого, $r_{i_1 i_2} + r_{i_2 i_3} + \dots + r_{i_n i_1}$, не превосходит r ?

Проверка до корня

Тест на простоту
12 нет

Факторизация 5000 лет
 $12=2*2*3$

В 2003 нашли полиномиальный алгоритм

Существует ли полиномиальный алгоритм - неизвестно

Чтобы расшифровать страницу - надо решить задачу факторизации (200 цифр в длину)
123642834691274812938461296741912431
 10^{70} лет, если использовать все компы на земле