

Как правильно раскладывать на множители (докуда проверять)

факторизации

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.

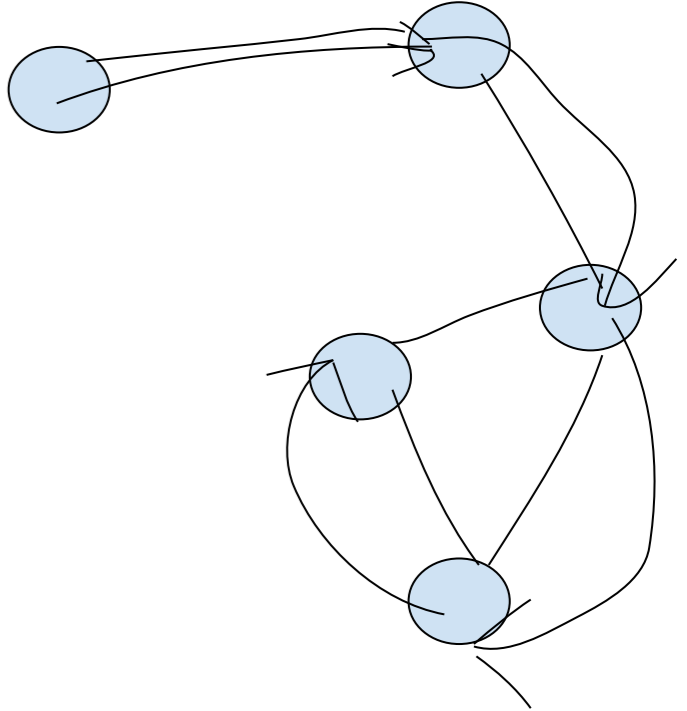
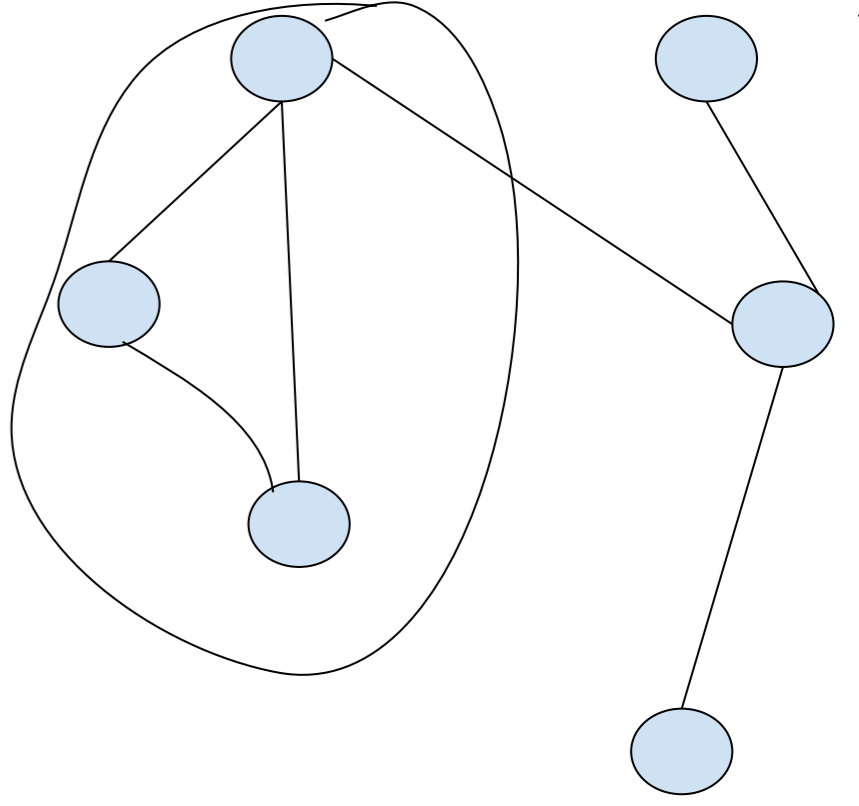
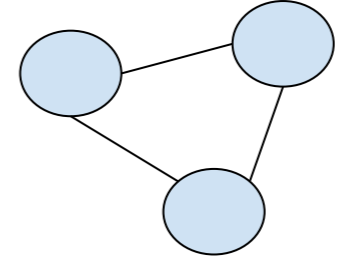
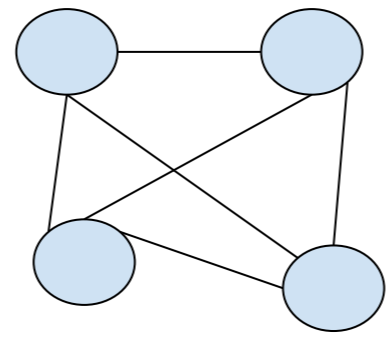
P=?=NP нерешенная проблема

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

Леня Левин 1970-ые СССР

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

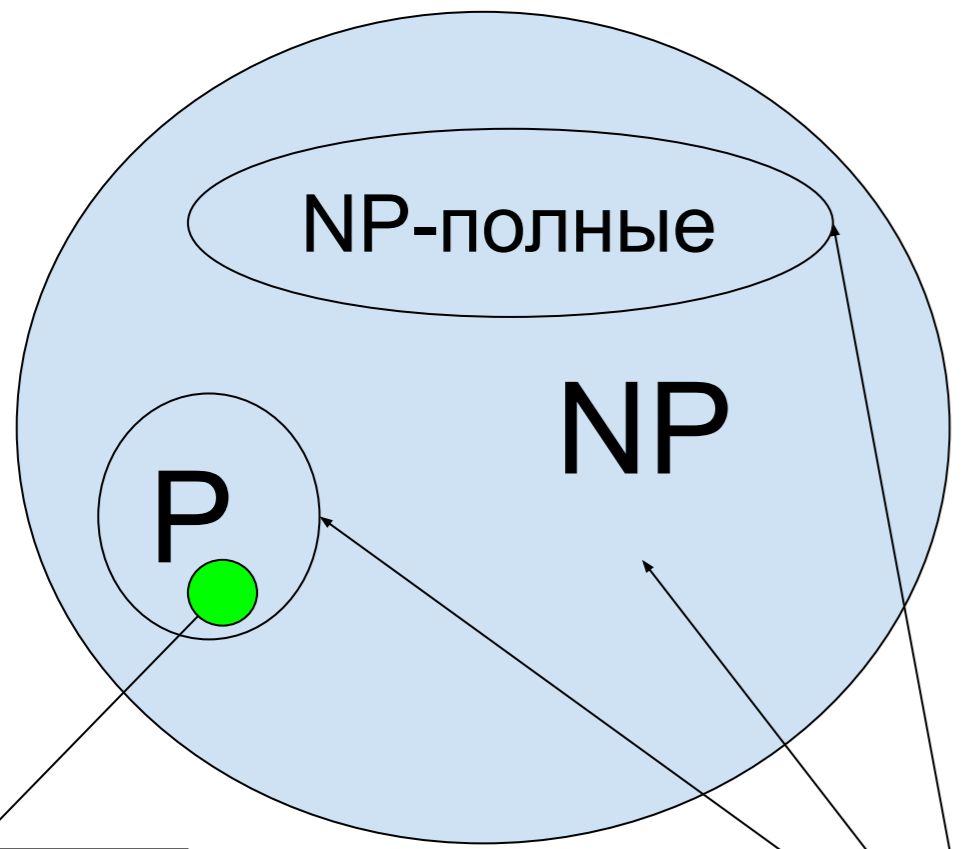
NP-задачи, решаемые полным перебором



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 ?

$y = ax^n + bx^{(n-1)} + \dots + cx + 1$ (многочлен = относительно быстро решаемая)
 $y = 2^x$ (показательная, экспоненциальная = долго решаемых полным перебором)

$y_1(x) = x^{100}$
 $y_2(x) = 100^x$
 $x = 1\,000\,000$
 $y_1(1\,000\,000) = 1\,000\,000^{100} = (10^6)^{100} = 10^{600}$
 $y_2(1\,000\,000) = 100^{1\,000\,000} = (10^2)^{1\,000\,000} = 10^{2\,000\,000}$



Тест на простоту

Факторизация ?