Как правильно раскладывать на множители (докуда проверять)

тест на простоту составного числа

факторизация (разложение на множители) составного числа

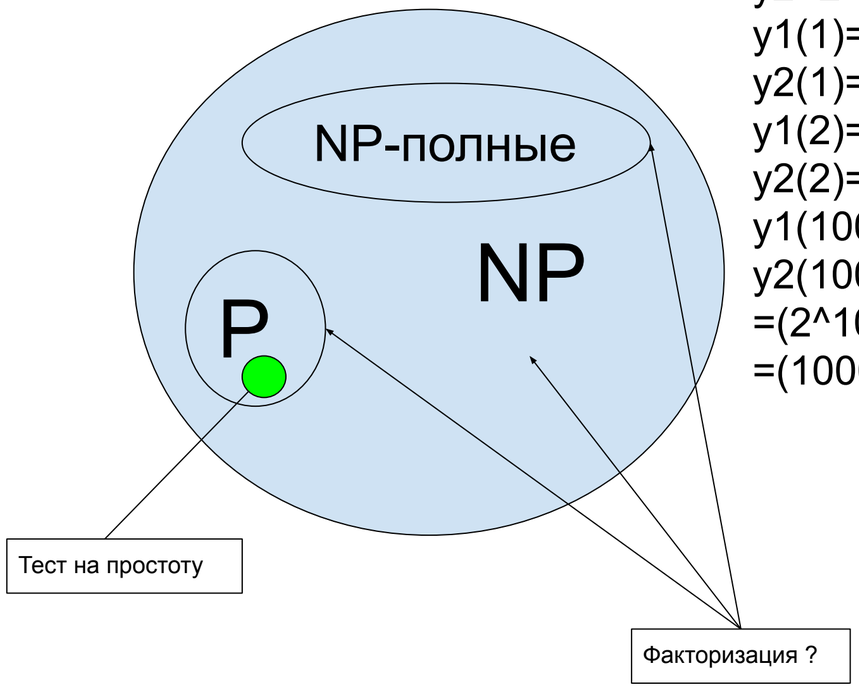
Разница факторизации и теста на простоту

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

P=?=NP 40 лет



y1=n^5+3n+1(полином)
y2=2^n(не полином)
y1(1)=5
y2(1)=2
y1(2)=39
y2(2)=4
y1(1000)=1000^5=10^15
y2(1000)=2^1000=
=(2^10)^100=(1024)^100
=(1000)^100=10^300

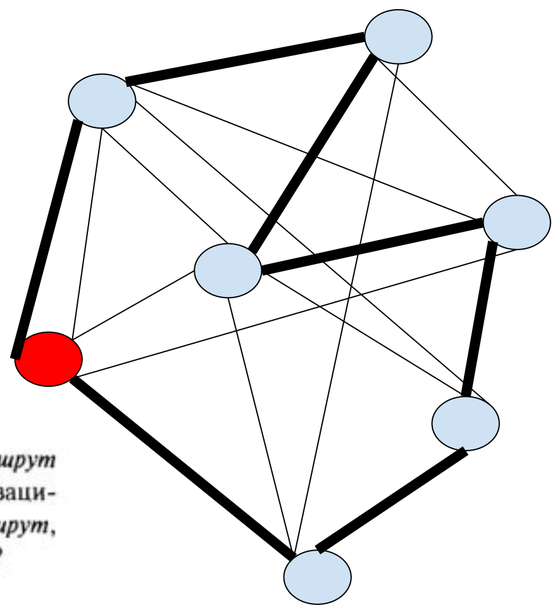
761
на 2, 3, 5, 7, 11, …
имеет ли смысл пытаться поделить 761 на 759
не имеет смысла проверять больше половины

есть понятие квадратный корень из числа

имеет смысл проверять до корня
V25=5 < V30 < V36=6
чему примерно равен корень 761=27…
пусть мы проверили все простые числа до 27 и 761 ни на одно из них не поделилось, мы начали дальше проверять, и - о чудо, например 761 поделилось на 41
761/41=x (17)
761=41*17
761 = 27*27 = 41* 17
52347853827 22347853827 538271

2 100-значных простых числа, ты их перемножишь получишь 200-значное составное ты за пару часов, калькулятор за долю секунды

чтобы по 200 -значному составному узнать простые множители методом перебора понадобится 10^83 лет



[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,* $r_{i_1 i_2} + r_{i_2 i_3} + \ldots + r_{i_n i_1}$, *не превосходит* r?