тест на простоту

в 2003 году японские математики эта задача является P-задачей

достаточно проверять делители до корня квадратного

разложение на множители (факторизация)

RSA
1970

3x-1=0 (всегда известно)
3x^2+x-1=0 (придумали 1000 лет назад)
3x^3-x + 7=0 (придумали 500 лет назад)
3x^4-x + 7=0 (придумали 450 лет назад)
еще 300 лет искали способ для ур-ий 5-ой степени

150 лет назад Эварист Галуа доказал, что формул для решений ур-ий 5-ой степени нет и быть не может

x^2007-3x=1

x^2

P-задачи

достаточно быстро есть алгоритмом, скорость работы которого описывается полиномом

полином=многочлен
y=3x^2+x-1
y=3x-1
y=3x^3-x + 7

x=3 объектов
y=3*3^2+3-1=29 операций

2^x

NP-задачи

нет алгоритма, скорость работы которого описывается полиномом

y=2^x

y=x^2	1	4	9	16	25	36	49		1000^2=1000 000=10^6
y=2^x	2	4	8	16	32	64	128		2^1000=(2^10)^100=(10^3)^100=10^300
x =	1	2	3	4	5	6	7	…	1000