



Problem 3. «Factoring in 2019»

Nicole is learning about the RSA cryptosystem. She has chosen random 500-bit prime numbers p and q , $2^{499} \leq p, q < 2^{500}$, and computed $n = p \cdot q$. Being a curious and creative person, she has also combined the three numbers in funny ways. Her favorite one is an integer h such that

$$h \equiv 3^{2019}p^2 + 5^{2019}q^2 \pmod{n^2 + 8 \cdot 2019}.$$

Unfortunately, she has lost the paper where she wrote the two prime numbers. Luckily, she remembers n and h . Help Nicole to recover p and q .

$n =$ 40763613025504836845249840044831561583564626405535158138667037
 18791672670905308860844304055285019651507728831663677166092475
 16155419756121537288444995708421977847213953345126368990185271
 10259760189356588305406519080647582874212687596214191915933827
 67252094717222418132289251314647500491996323400002019,

$h =$ 78307999278336577586961528110240026923828914927526911949501196
 64549497756373569985393554661132717198368717093111812566649031
 17342818449633588647098544612151278035131454234786653136500887
 08830470996542888912418213532073622903727205396807848603735835
 72653630883685906916701587362236649126895719656663293825501223
 97088799629252601249428062432254738935764304610281613264225641
 74990272864680012560095992125783832230234589257650929348364268
 48117494065463529201859600747521892957258104033195441014023432
 36581529201392185327635674923459290749241831590661903965132514
 2154451518308886658505820006667836934411881.