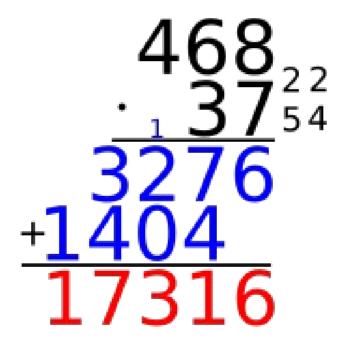
Multiplication is polynomial time in number of digits $(O(n^2) \text{ or } O(n \log n))$



Modular exponentiation

153¹⁸⁹ (mod 251)

Naive way: multiply 153 times itself 189 times. Won't work for, *e.g.*, 2048-bit numbers, especially for the exponent

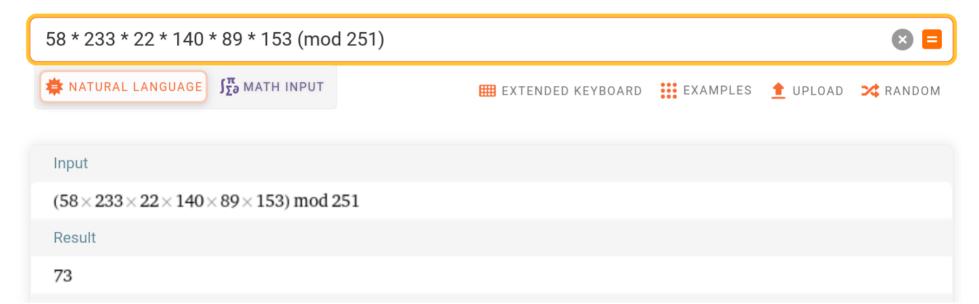
Better way (all mod 251)

$$153^{0} = 1$$
 $153^{8} = 140$
 $153^{1} = 153$ $153^{16} = 22$
 $153^{2} = 66$ $153^{32} = 233$
 $153^{4} = 89$ $153^{64} = 73$
 $153^{128} = 58$

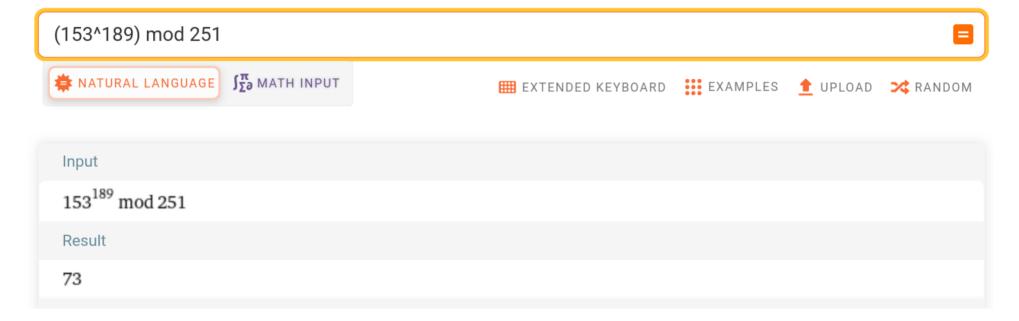
Better way

- 189 in binary is 0b10111101
- $189 = 1^{27} + 0^{26} + 1^{25} + 1^{24} + 1^{23} + 1^{22} + 0^{21} + 1^{20}$
- $153^{189} \pmod{251} = 153^{(128+0+32+16+8+4+0+1)} \pmod{251}$
 - $= 153^{128} * 153^{32} * 153^{16} * 153^{8} * 153^{4} * 153^{1} \pmod{251}$
 - = 58 * 233 * 22 * 140 * 89 * 153 (mod 251)
 - = 73

WolframAlpha computational intelligence.







$153^{189} = 73 \pmod{251}$ $189 = \log_{153} 73 \pmod{251}$

This is called the discrete logarithm, and there is no known algorithm for solving it in the general case that is polynomial in the number of digits.

$153^{189} = 73 \pmod{251}$ $153^{64} = 73 \pmod{251}$

$153^{189} \equiv 73 \pmod{251}$ $153^{64} \equiv 73 \pmod{251}$

$153^{189} \equiv 153^{64} \equiv 73 \pmod{251}$