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

$$468 \cdot 37$$

$$3276$$
$$+1404$$
$$17316$$

Modular exponentiation

153^{189} (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)

$153^0 = 1$

$153^1 = 153$

$153^2 = 66$

$153^4 = 89$

$153^8 = 140$

$153^{16} = 22$

$153^{32} = 233$

$153^{64} = 73$

$153^{128} = 58$

Better way

- 189 in binary is 0b10111101

- $189 = 1 \cdot 2^7 + 0 \cdot 2^6 + 1 \cdot 2^5 + 1 \cdot 2^4 + 1 \cdot 2^3 + 1 \cdot 2^2 + 0 \cdot 2^1 + 1 \cdot 2^0$

- $153^{189} \pmod{251} = 153^{(128+0+32+16+8+4+0+1)} \pmod{251}$

  $= 153^{128} \cdot 153^{32} \cdot 153^{16} \cdot 153^8 \cdot 153^4 \cdot 153^1 \pmod{251}$

  $= 58 \cdot 233 \cdot 22 \cdot 140 \cdot 89 \cdot 153 \pmod{251}$

  $= 73$

WolframAlpha computational intelligence™

58 * 233 * 22 * 140 * 89 * 153 (mod 251)

NATURAL LANGUAGE   ∫π∑∂ MATH INPUT

EXTENDED KEYBOARD   EXAMPLES   UPLOAD   RANDOM

Input

$(58 \times 233 \times 22 \times 140 \times 89 \times 153) \bmod 251$

Result

73

WolframAlpha computational intelligence™

(153^189) mod 251

Input

$$153^{189} \bmod 251$$

Result

73

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

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

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.

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

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

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