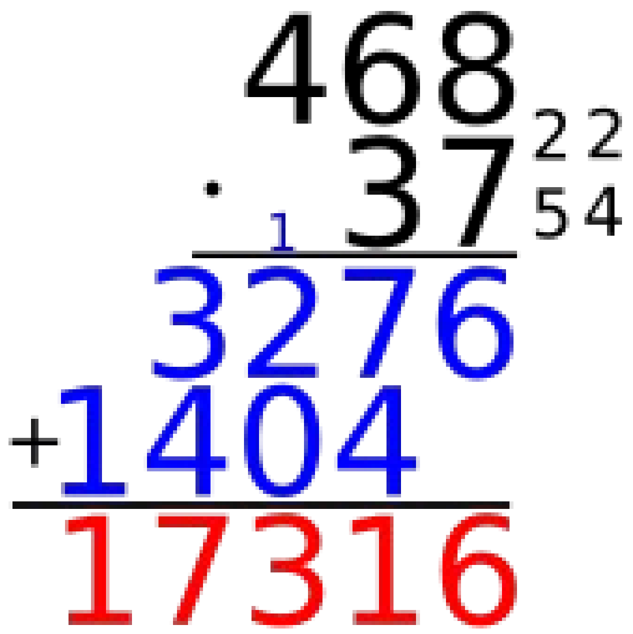
Multiplication is polynomial time in number of digits ($O(n^2)$ or $O(n \log n)$)



Modular exponentiation

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

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
- $189 = 1*2^7 + 0*2^6 + 1*2^5 + 1*2^4 + 1*2^3 + 1*2^2 + 0*2^1 + 1*2^0$
- $153^{189} \pmod{251} = 153^{(128+0+32+16+8+4+0+1)} \pmod{251}$

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

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

  $= 73$

WolframAlpha computational intelligence.

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

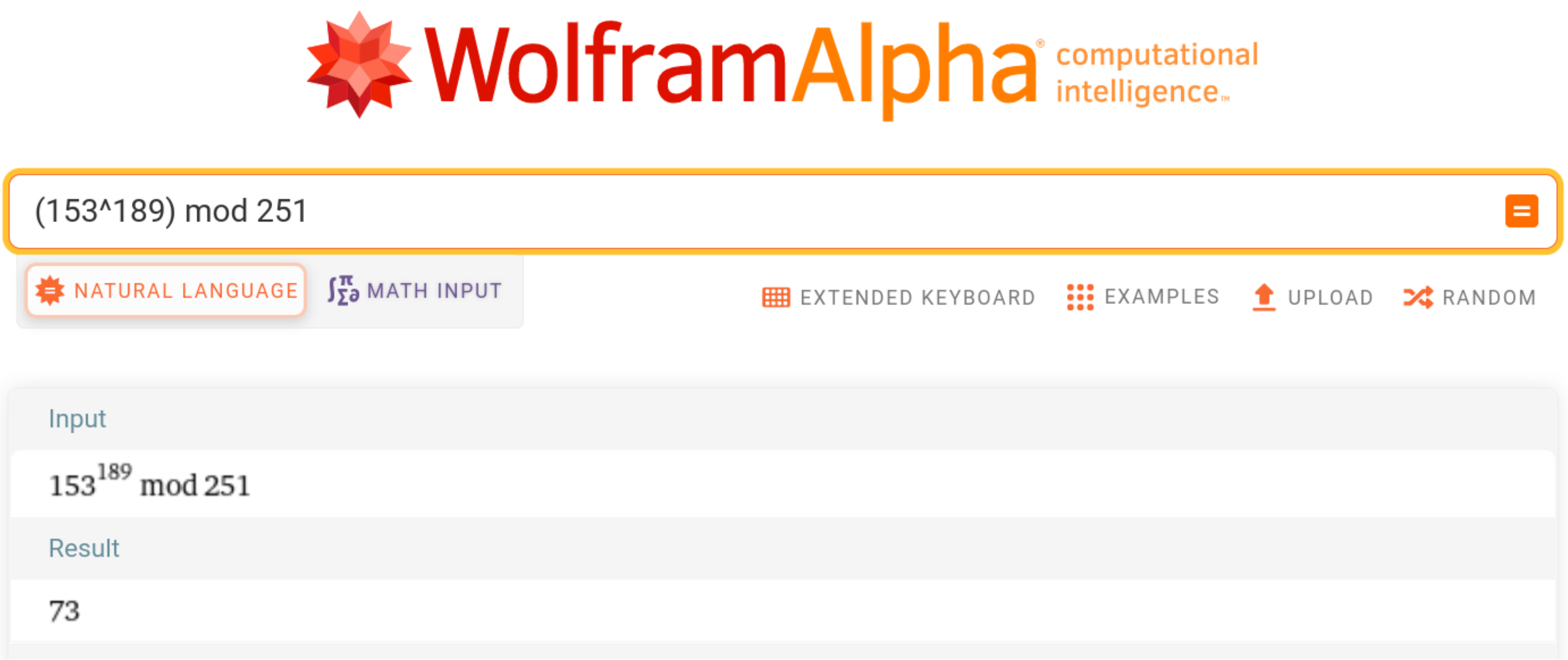
NATURAL LANGUAGE   MATH INPUT   EXTENDED KEYBOARD   EXAMPLES   UPLOAD   RANDOM

Input

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

Result

73


WolframAlpha computational intelligence.
(153^189) mod 251
NATURAL LANGUAGE
MATH INPUT
EXTENDED KEYBOARD
EXAMPLES
UPLOAD
RANDOM
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.

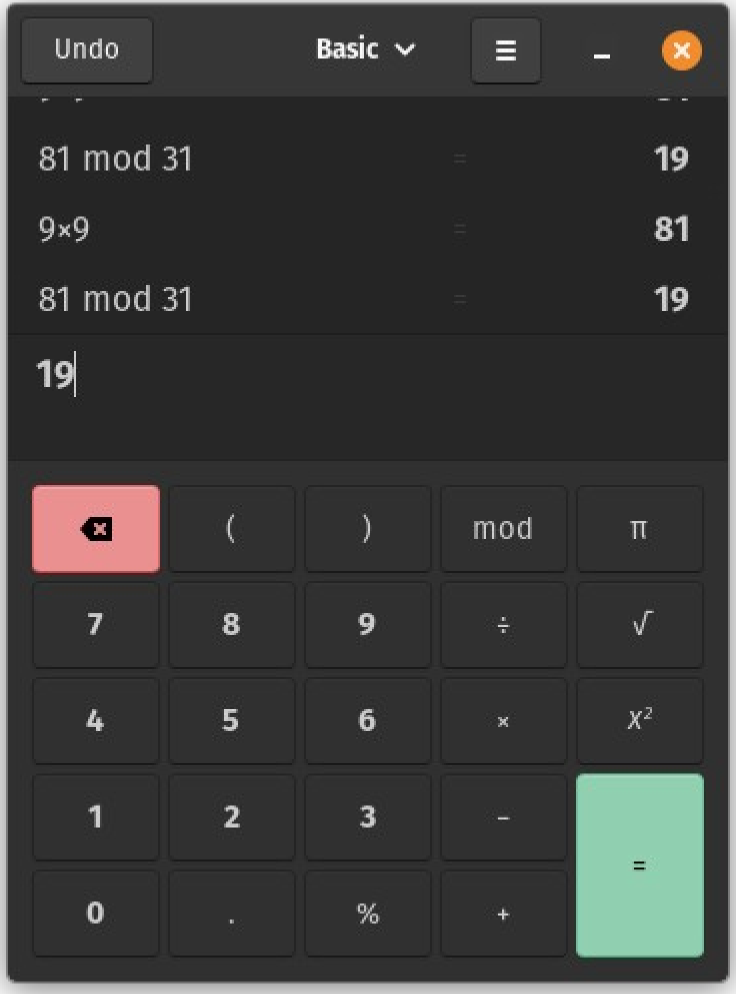
$$153^{189} = 73 \pmod{251}$$
$$153^{64} = 73 \pmod{251}$$

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

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

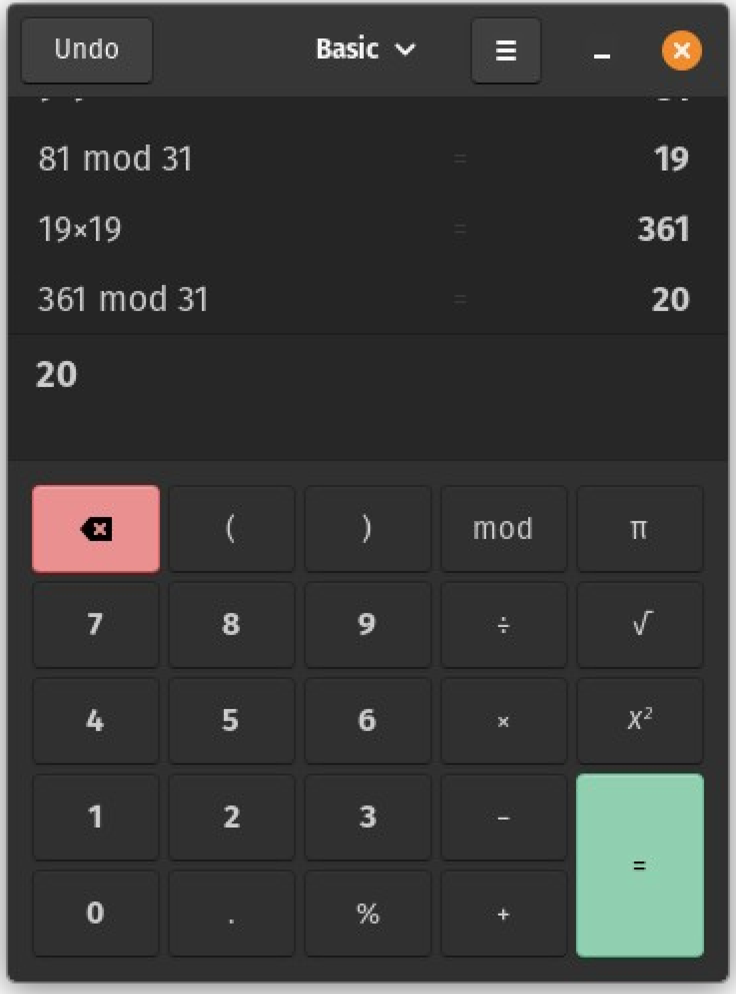
An example…

- 3^{17} mod 31
- 17 = 16 + 1
- 16 = 2^4 , $(((3^2)^2)^2)^2=3^{16}$
- All mod 31…
  - $3^1=3$, $3^2=9$, …


Undo
Basic
81 mod 31 = 19
9×9 = 81
81 mod 31 = 19
19
( ) mod π
7 8 9 ÷ √
4 5 6 × x²
1 2 3 − =
0 . % +

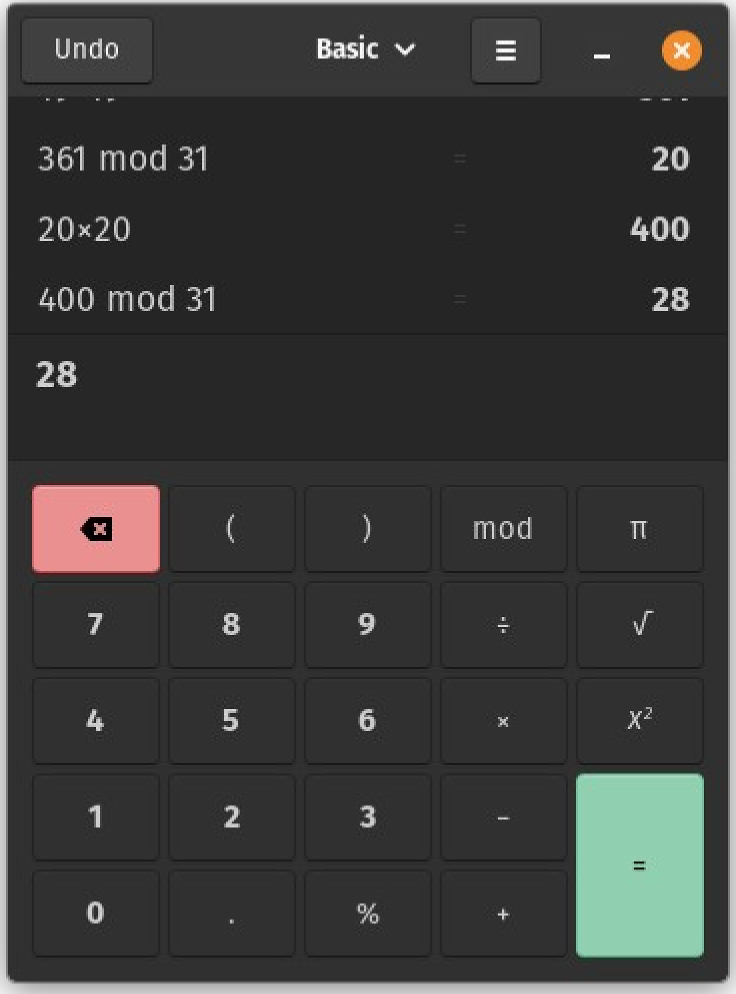
An example…

- 3^{17} mod 31
- 17 = 16 + 1
- $16 = 2^4$, $(((3^2)^2)^2)^2=3^{16}$
- All mod 31…
  - $3^1=3$, $3^2=9$, $3^4=19$, …


Undo
Basic
81 mod 31
19
19×19
361
361 mod 31
20
20
(
)
mod
π
7
8
9
÷
√
4
5
6
×
x²
1
2
3
−
=
0
.
%
+

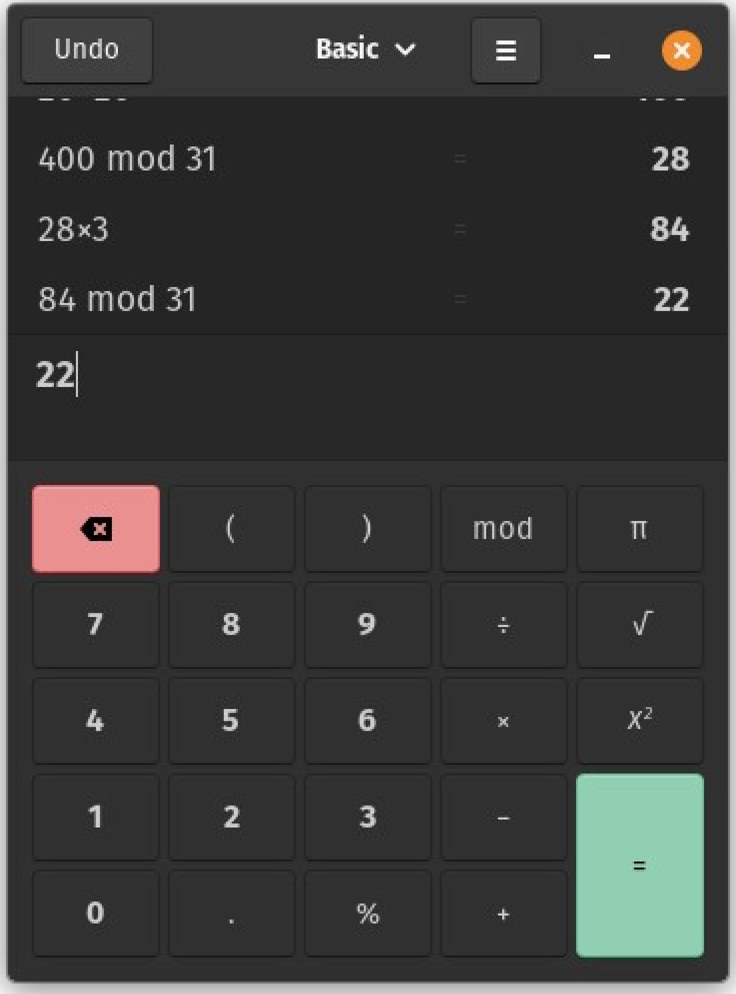
An example…

- 3^{17} mod 31
- $17 = 16 + 1$
- $16 = 2^4$, $(((3^2)^2)^2)^2=3^{16}$
- All mod 31…
  - $3^1=3$, $3^2=9$, $3^4=19$, $3^8=20$, …


Undo
Basic
361 mod 31 = 20
20×20 = 400
400 mod 31 = 28
28
( ) mod π
7 8 9 ÷ √
4 5 6 × x²
1 2 3 −
0 . % + =

An example…

- 3^{17} mod 31
- $17 = 16 + 1$
- $16 = 2^4$, $(((3^2)^2)^2)^2=3^{16}$
- All mod 31…
  - $3^1=3$, $3^2=9$, $3^4=19$, $3^8=20$, $3^{16}=28$…


Undo
Basic
400 mod 31 = 28
28×3 = 84
84 mod 31 = 22
22
( ) mod π
7 8 9 ÷ √
4 5 6 × x²
1 2 3 −
0 . % + =

An example…

- 3^{17} mod 31 $= 3^{16}3^{1}$ mod 31 = 22
- 17 = 16 + 1
- $16 = 2^4$, $(((3^2)^2)^2)^2=3^{16}$
- All mod 31…
  - $3^1=3$, $3^2=9$, $3^4=19$, $3^8=20$, $3^{16}=28$…

17 in binary is 0b10001