Problem 2

Find the integer A satisfying

$$2^{63} \equiv \mathbf{A} \pmod{131} \qquad 0 \le A \le 130.$$

Find the minimum positive integer B satisfying

$$3^{\mathbf{B}} \equiv 26 \pmod{31}.$$

- 131, 31 are prime numbers.
- Calculation of A is easy.
- Calculation of B is more difficult!

(**Discrete Logarithm Problem**)

Problem 2

Calculation of $2^{63} \equiv$ A (mod 131)

$$2^{63} = 9223372036854775808$$
$$\equiv 98 \pmod{131}$$

Problem 2

Calculation of $2^{63} \equiv A \pmod{131}$

$$2^8 \equiv (2^4)^2 \equiv 16 \times 16 \equiv 125$$

$$2^{16} \equiv (2^8)^2 \equiv 125 \times 125 \equiv 36$$

$$2^{32} \equiv (2^{16})^2 \equiv 36 \times 36 \equiv 117$$

$$2^{64} \equiv (2^{32})^2 \equiv 117 \times 117 \equiv 65$$

$$2 \times 66 = 132 \equiv 1$$

$\Rightarrow$ 66 is the **multiplicative inverse** to 2

$$2^{63} \equiv 66 \times 2^{64} \equiv 66 \times 65 \equiv \mathbf{98}$$

Problem 2

- Calculation of B satisfying
  $3^{B} \equiv 26 \pmod{31}$ is more difficult.
  (**Discrete Logarithm Problem**)

  $3^3 \equiv 27$

  $3^4 \equiv 27 \times 3 \equiv 81 \equiv 19$

  $3^5 \equiv 19 \times 3 \equiv 57 \equiv 26$

Answer B = 5