Problem 4

Find A,B, and C.

$$2^{1000} \equiv A \pmod{13} \qquad 0 \le A \le 12$$

$$21! \equiv B \pmod{23} \qquad 0 \le B \le 22$$

$$C = \text{mult inverse to } 17 \pmod{81}$$

$$1 \le C \le 80$$

$$2^{1000} = 2 \times 2 \times \cdots \times 2 \ \ (1000 \text{ times}) = ???$$

$$21! = 1 \times 2 \times 3 \times \cdots \times 21$$

$$= 51090942171709440000 \ \ (\text{too big})$$

Problem 4

- How can we calculate $2^{1000} \pmod{13}$?
- By **Fermat's Little Thm**,

$$2^{12} \equiv 1 \pmod{13}$$

Therefore,

$$\begin{aligned} 2^{1000} &\equiv 2^{12\times 83+4} \\ &\equiv (2^{12})^{83} \times 2^4 \\ &\equiv 2^4 \equiv 16 \\ &\equiv \mathbf{3} \pmod{13} \end{aligned}$$

Pierre de Fermat
(1607?-1665)

Problem 4

- How can we calculate $21! \pmod{23}$?
- By **Wilson's Thm**,

$$22! = 1\times 2\times 3\times \cdots \times 22 \equiv -1 \pmod{23}$$

Therefore,

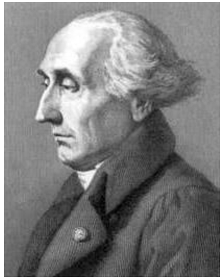
$$21! \times 22 \equiv -1$$

Since $22 \equiv -1$,

$$21! \times (-1) \equiv -1$$

$$\Rightarrow 21! \times (-1)^2 \equiv (-1)^2$$

$$\Rightarrow 21! \equiv \mathbf{1}$$



Joseph-Louis Lagrange (1736-1813)

https://en.wikipedia.org/wiki/Joseph-Louis_Lagrange

Problem 4

- How can we find C ?

  C = **multiplicative inverse** to 17 (mod 81)

  $C \times 17 \equiv 1 \pmod{81}$

- Use **Euclidean Algorithm** !

Euclid of Alexandria (fl. 300BC)

https://en.wikipedia.org/wiki/Euclid

Problem 4

Euclidean Algorithm GCD(17,81)=1

$$81 = 4\times17 + 13 \Rightarrow \mathbf{13} = 81 - 4\times17$$

$$17 = 13 + 4 \Rightarrow \mathbf{4} = 17 - \mathbf{13}$$

$$13 = 3\times4 + 1 \Rightarrow 1 = \mathbf{13} - 3\times\mathbf{4}$$

Therefore,

$$1 = \cdots = 4\times81 - 19\times17$$

$$1 \equiv -19\times17 \equiv \mathbf{62}\times17 \pmod{81}$$

Answer C=62

Euclid of Alexandria (fl. 300BC)

Problem 4

- If A, B are **relatively prime** (GCD(A,B)=1)

$$\mathbf{A \times C + B \times D = 1}$$

for some C and D.

$$\Rightarrow \mathbf{A \times C \equiv 1 \pmod{B}}.$$

- We can calculate mult inverse using **Euclidean Algorithm**.

Euclid of Alexandria (fl. 300BC)