Problem 4

Calculate

$$2^{560}, \quad 3^{560}, \quad 5^{560}, \quad 7^{560} \pmod{561}$$

(Hint: $561 = 3\times 11\times 17$)

$$\begin{aligned}2^{560} = \ &377396242482154135224155458098826889\\&091692122041644042837620630024562416\\&239214885208612672517765876754146837\\&503076384489977058462992479263256143\\&42514326960436493953269 76\end{aligned}$$

$$\equiv \ \mathbf{???} \pmod{561}$$

Problem 4

- Can we calculate $A^{560} \pmod{561}$?
- We cannot use **Fermat's Little Thm** because $561 = 3\times11\times17$ is **not a prime number**.

Claim $A \equiv B \pmod{561}$ **if and only if**

$A \equiv B \pmod{3}$,

$A \equiv B \pmod{11}$, and

$A \equiv B \pmod{17}$.

Problem 4

Proof of Claim ($561 = 3\times11\times17$)

$A\equiv B \pmod{561}$

$\Leftrightarrow$ $A-B$ is divisible by 561.

$\Leftrightarrow$ $A-B$ is divisible by 3, 11, and 17.

$\Leftrightarrow$ $A\equiv B \pmod 3$, $A\equiv B \pmod{11}$, and $A\equiv B \pmod{17}$.

- We need to calculate $\mathbf{A^{560} \pmod N}$ for $N=3, 11, 17$.

Problem 4

- **(mod 3)** By **Fermat's Little Thm**,
  $A^2 \equiv 1 \pmod 3$ if A is not divisible by 3.
  $A^{560} = (A^2)^{280} \equiv 1^{280} \equiv \mathbf{1 \pmod 3}$.
- **(mod 11)** If A is not divisible by 11,
  $A^{560} = (A^{10})^{56} \equiv 1^{56} \equiv \mathbf{1 \pmod{11}}$.
- **(mod 17)** If A is not divisible by 17,
  $A^{560} = (A^{16})^{35} \equiv 1^{35} \equiv \mathbf{1 \pmod{17}}$.
  $(560 = 16 \times 35)$

Problem 4

Conclusion

If A and 561 are relatively prime (GCD(A,561)=1),

$$\mathbf{A^{560} \equiv 1 \pmod{561}}.$$

Answer $2^{560} \equiv 5^{560} \equiv 7^{560} \equiv 1 \pmod{561}$

- How can we calculate $3^{560} \pmod{561}$?

Problem 4

$3^{560} \equiv \mathbf{0} \pmod{3}$, $3^{560} \equiv \mathbf{1}$ (mod 11, 17).

By **Chinese Remainder Thm**, there is a **unique** A ($0 \le A \le 560$) satisfying

$A \equiv 0 \pmod{3}$, $A \equiv 1$ (mod 11, 17).

In fact, $A = 375$.

Answer $3^{560} \equiv 375 \pmod{561}$

Problem 4

- If A and 561 are **relatively prime** (GCD(A,561)=1),

$$A^{560} \equiv 1 \pmod{561}.$$

- 561 is an example of **Carmichael Numbers**. It is also an example of **pseudo-prime numbers**.