Problem 2

Choose all the correct statements. (Multiple choices)

(a) 83 is QR (mod 503).
(b) 83 is not QR (mod 503).
(c) 503 is QR (mod 83).
(d) 503 is not QR (mod 83).

- **QR** = Quadratic Residue
- Use the **Quadratic Reciprocity Law** (**QRL**).

Carl Friedrich Gauss (1777-1855)

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

Problem 2

- (Recall) A is **QR (mod P)** if

  $\mathbf{A \equiv X^2 \pmod{P}}$ for some X.

$83 \equiv Y^2 \pmod{503}$ for some Y?

$503 \equiv Z^2 \pmod{83}$ for some Z?

- We can solve these problems using the **Quadratic Reciprocity Law**.

Carl Friedrich Gauss (1777-1855)

Problem 2

Quadratic Reciprocity Law

$P \neq Q$ **odd** prime numbers

(1) If **$P \equiv 1$ or $Q \equiv 1 \pmod 4$**,

P is QR (mod Q)

$\Leftrightarrow$ **Q is QR** (mod P).

(2) If **$P \equiv Q \equiv 3 \pmod 4$**,

P is QR (mod Q)

$\Leftrightarrow$ **Q is not QR** (mod P).

- Use QRL for P=83, Q=503.

Carl Friedrich Gauss (1777-1855)

Problem 2

$83 \equiv 3,\ \ 503 \equiv 3 \pmod 4$,

- Assume **83 is QR (mod 503).**
- By QRL,

  83 is QR (mod 503)

  $\Leftrightarrow$ 503 is **non-QR** (mod 83)

  $\Leftrightarrow$ 5 is **non-QR** (mod 83)

$(503 = 6\times83+5 \equiv 5 \pmod{83})$

- Apply QRL again!

Carl Friedrich Gauss (1777-1855)

Problem 2

$5 \equiv 1,\ \ 83 \equiv 3 \pmod 4$,

- By QRL,

  5 is **non-QR** (mod 83)

  $\Leftrightarrow$ 83 is **non-QR** (mod 5)

  $\Leftrightarrow$ 3 is **non-QR** (mod 5)

  $(83 = 16 \times 5 + 3 \equiv 3 \pmod 5)$

- This assertion is true because

  3 is not QR (mod 5).

Carl Friedrich Gauss (1777-1855)

Problem 2

Answer

The correct statements are

(a) 83 is QR (mod 503).
(d) 503 is not QR (mod 83).

In fact, $83 \equiv 33^2 \pmod{503}$.

Carl Friedrich Gauss (1777-1855)