

153

(a) What are quadratic residues and quadratic non-residues (mod 13)

$$1^2 = 1, 2^2 = 4, 3^2 = 9, 4^2 = 3, 5^2 = 12$$

$$6^2 = 10, 7^2 = 10, 8^2 = 12, 9^2 = 3, 10^2 = 9$$

$$11^2 = 4, 12^2 = 1$$

Q res: 1, 3, 4, 9, 10, 12

Non Q res: 2, 5, 6, 7, 8, 11

(b) For each quadratic residues in \mathbb{Z}_{13}^* what are its square roots

* Check

* Rec-co

$$\mathbb{Z}_{13}^* = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12\}$$

$$1, 4, 9, 16, 25, 36, 49, 64, 81, 100, 121, 144$$

$$x^2 \equiv 1 \pmod{13} \Rightarrow x = 1 \text{ or } 12$$

$$x^2 \equiv 3 \pmod{13} \Rightarrow x = 4 \text{ or } 9$$

$$x^2 \equiv 4 \pmod{13} \Rightarrow x = 2 \text{ or } 11$$

$$x^2 \equiv 9 \pmod{13} \Rightarrow x = 3 \text{ or } 10$$

$$x^2 \equiv 10 \pmod{13} \Rightarrow x = 6 \text{ or } 7$$

$$x^2 \equiv 12 \pmod{13} \Rightarrow x = 5 \text{ or } 8$$

$$\sqrt{1} = 1, 12$$

$$\sqrt{12} = 5, 8$$

$$\sqrt{3} = 4, 9$$

$$\sqrt{4} = 2, 11$$

$$\sqrt{9} = 3, 10$$

$$\sqrt{10} = 6, 7$$