Quiz #3

MATH 481/581 — Cryptography
Monday, Feb 13

Please print your name:

Problem 1. List all quadratic residues modulo 11.

Solution. We compute all squares: $0^2 = 0$, $(\pm 1)^2 = 1$, $(\pm 2)^2 = 4$, $(\pm 3)^2 = 9$, $(\pm 4)^2 \equiv 5$, $(\pm 5)^2 = 3$. Hence, the quadratic residues modulo 11 are $0, 1, 3, 4, 5, 9$. □

Problem 2. How many invertible quadratic residues are there modulo 505? (101 is a prime.)

Solution. $\frac{1}{4}\phi(505) = \frac{1}{4} \cdot 4 \cdot 100 = 100$ □

Problem 3.

(a) Using the Chinese remainder theorem, solve $x \equiv 2 \pmod{5}$, $x \equiv 9 \pmod{11}$. (Steps needed for full credit.)

(b) Using your answer from the first part, determine all solutions to $x^2 \equiv 4 \pmod{55}$.

Solution.

(a) $x \equiv 2 \cdot 11 \cdot \underbrace{11^{-1}_{\text{mod } 5}}_{1} + 9 \cdot 5 \cdot \underbrace{5^{-1}_{\text{mod } 11}}_{-2} = 22 - 90 \equiv 42 \pmod{55}$

(b) By the CRT:

$$\begin{aligned} & x^2 \equiv 4 \pmod{55} \\ \Longleftrightarrow\ & x^2 \equiv 4 \pmod{5} \text{ and } x^2 \equiv 4 \pmod{11} \\ \Longleftrightarrow\ & x \equiv \pm 2 \pmod{5} \text{ and } x \equiv \pm 2 \pmod{11} \end{aligned}$$

By the first part, $x \equiv 2 \pmod{5}$, $x \equiv -2 \pmod{11}$ has the solution $x \equiv 42 \equiv -13 \pmod{55}$.

Hence, we conclude that $x^2 \equiv 4 \pmod{55}$ has the four solutions $\pm 2, \pm 13 \pmod{5}$.

□

Armin Straub
straub@southalabama.edu