Homework 8

Question 1

Let $p = 179$.

For each of the following values of x, is x a quadratic residue modulo p? Justify your answer.

a) $x = 27$

b) $x = 147$

Question 2

Let $N = 173 \times 179 = 30967$

For each of the following values of x, is x a quadratic residue modulo N? Justify your answer.

a) $x = 206$

b) $x = 4980$

Question 3

(i) Let $p = 17$ (a prime)

a) what is $p \bmod 4$?

b) Is $p-1$ a quadratic residue mod p?

Why?

(ii) Let $p = 11$ (a prime)

a) what is $p \bmod 4$?

b) Is $p-1$ a quadatic residue mod p?

Why?

(iii) Let p be a odd prime.

$p-1$ is a quadatic residue mod p

iff $p \equiv ? \bmod 4$.

Prove it.

Question 4

Solve b such that $b^2 \equiv c \pmod{p}$ where $p \equiv 3 \pmod{4}$ for the following values.

(i) Solve $b^2 \equiv 116 \pmod{587}$.

(ii) Solve $b^2 \equiv 3217 \pmod{8627}$.

(iii) Solve $b^2 \equiv 9109 \pmod{10663}$.

Show how you compute the values of b without using brute-force.

There are suppose to be two square roots, hence provide two values of b for each of the questions.

Question 5

$N = pq$ is called a **Blum integer** if p and q are distinct odd primes with $p \equiv q \equiv 3 \bmod 4$.

For each of the following Blum integers N compute the square roots of x, which is a quadratic residue modulo N.

Note: There are four square roots!

(a) $N = 179 \times 191$, $x = 20$

(b) $N = 179 \times 283$, $x = 15$

For each of four square roots of $x \bmod N$, which one of them is a quadratic residue mod N?