4400-001 - SPRING 2022 - WEEK 9 (3/15, 3/17)
SQUARES MOD p

Some of these exercises can be found in Savin - Chapter 6.

Exercise 1 (required). Squares mod p.

(1) For each odd prime $p \leq 31$, identify all of the squares and non-squares in $\mathbb{F}_p$.
(2) For p an odd prime, how many non-zero squares are there in $\mathbb{F}_p$?
Give a logical explanation for your answer.

Exercise 2. Patterns in squares mod p.

(1) Based on 1-(1), can you guess a pattern for when -1 is a square in $\mathbb{F}_p$?
(2) Based on 1-(1), can you guess a pattern for when 2 is a square in $\mathbb{F}_p$?
(3) Using the data from 1-(1), compare for primes p and q when p is a square mod q and when q is a square mod p. Do you notice any patterns?

Exercise 3 (required). Using the Legendre symbol. For p a prime and $n \in \mathbb{Z}$ with $p \nmid n$, the Legendre symbol is defined by

$$\left(\frac{n}{p}\right) = \begin{cases} 1 & \text{if } n \text{ is a square mod } p \\ -1 & \text{if } n \text{ is not a square mod } p \end{cases}$$

In the lecture for Thursday we will discuss this further and introduce some rules for computing the Legendre symbol; use these properties to complete the following exercises.

(1) Is 66 a square mod 127?
(2) Is 80 a square mod 127?
(3) Compute $\left(\frac{122}{127}\right)$.
(4) For which odd primes p is 5 a square mod p?
(5) For which odd primes p is 3 a square mod p?

Exercise 4. Primes congruent to $1 \mod 4$**.**

(1) Let n be a positive integer and let p be a prime divisor of $n^2 + 1$. Show that $p \equiv 1 \mod 4$.
Hint: consider $\left(\frac{n^2}{p}\right)$.
(2) Use part (1) to show that there infinitely many primes $p \equiv 1 \mod 4$.

Exercise 5. Primes congruent to $1 \mod 3$**.**

(1) Let n be a positive integer and let p be a prime divisor of $n^2 + 3$. Show that $p \equiv 1 \mod 3$.
Hint: consider $\left(\frac{n^2}{p}\right)$.
(2) Use part (1) to show that there infinitely many primes $p \equiv 1 \mod 3$.

Exercise 6. For integer primes p and q, what can you say about when q is a square in $\mathbb{Z}[i]/(p)$?