4400-001 - SPRING 2022 - WEEK 10 (3/22, 3/24)
EXPLAINING QUADRATIC RECIPROCITY

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

Exercise 1 (required). More computations with squares mod p.

(1) Use the formula $\left(\frac{n}{p}\right) = n^{\frac{p-1}{2}} \mod p$ to determine if the following are squares. You may use a calculator; double-check your answers using the rules for the Legendre symbol (but you do not have to include this double-check in your homework that you turn in).

(a) $2 \mod 31$

(b) $2 \mod 43$

(c) $3 \mod 31$

(d) $7 \mod 29$

(2) Use the discrete logarithm with base $g = 3$ to find the square roots of 5 in $\mathbb{F}_{19}$.

(3) Which of the following equations have solutions? *Hint: complete the square.*

(a) $x^2 + 4x + 11 = 0 \mod 43$

(b) $x^2 - 6x + 11 = 0 \mod 131$

(c) $x^2 - 6x + 28 = 0 \mod 131$

Exercise 2 (required). Roots of unity and square roots

An *nth root of unity* in a field $\mathbb{K}$ is an element $\zeta \in \mathbb{K}$ such that $\zeta^n = 1$.
An nth root of unity ζ is *primitive* if $\zeta^d \neq 1$ for any proper divisor d of n.
In the following, Euler's identity $e^{i\theta} = \cos(\theta) + i\sin(\theta)$ may be helpful!

(1) Show that $\zeta_n := e^{2\pi i/n}$ is a primitive nth root of unity in $\mathbb{C}$.

(2) Verify that $(\zeta_3 - \zeta_3^2)^2 = -3$ in $\mathbb{C}$.

(3) Verify that $(\zeta_8 + \zeta_8^7)^2 = 2$ in $\mathbb{C}$.

(4) Verify that $(\zeta_5 + \zeta_5^4 - \zeta_5^2 - \zeta_5^3)^2 = 5$ in $\mathbb{C}$.

(5) Explain why $\mathbb{F}_p$ contains a primitive nth root of unity if and only if $p \equiv 1 \mod n$.
Hint : Use the discrete log.

(6) Find a primitive third root of unity $\zeta \in \mathbb{F}_7$, then verify by direct computation that
$$(\zeta^2 - \zeta)^2 = -3 \text{ in } \mathbb{F}_7$$

(7) Find a primitive eight root of unity $\zeta \in \mathbb{F}_{17}$, then verify by direct computation that
$$(\zeta + \zeta^7)^2 = 2 \text{ in } \mathbb{F}_{17}.$$

(8) Find a primitive fifth root of unity $\zeta \in \mathbb{F}_{11}$, then verify by direct computation that
$$(\zeta + \zeta^4 - \zeta^2 - \zeta^3)^2 = 5 \text{ in } \mathbb{F}_{11}.$$

(9) (Challenge, not to turn in). The formulas for square roots of -3 and 5 above are special cases of the following formula, due to Gauss: for ℓ an odd prime and ζ a primitive ℓth root of unity,
$$\left(\sum_{a=1}^{\ell-1}\left(\frac{a}{\ell}\right)\zeta^a\right)^2 = \left(\frac{-1}{\ell}\right)\cdot \ell.$$
Check this for some more values of ℓ and primitive roots of unity, e.g. in $\mathbb{F}_p$ and $\mathbb{C}$.

(10) (Challenge, not to turn in).
(a) Show $(\zeta - \zeta^2)^2 = -3$ for *any* primitive third root of unity ζ in any field.
Hint: use polynomial division to show that the primitive 3rd roots of unity are exactly the roots of $x^2 + x + 1$, then apply this to simplify the expansion of $(\zeta - \zeta^2)^2$.
(b) Show $(\zeta_5 + \zeta_5^4 - \zeta_5^2 - \zeta_5^3)^2 = 5$ for *any* primitive fifth root of unity ζ in any field.
(c) Show $(\zeta - \zeta^7)^2 = 2$ for *any* primitive eighth root of unity ζ in any field.