Math 3320 Homework Assignment #12

Due in class Wednesday December 3 and Friday December 5

Problems for Wednesday:

A: Use Pepin’s test to show that \( F_4 = 2^{2^4} + 1 \) is prime.
B: Show that \( F_n \equiv 2 \pmod{5} \).
C: Let \( G \) be a finite group with identity element \( e \). Suppose \( g^{2m-1} \neq e, g^m = e \). Show that the order of \( g \) must be \( 2m \).
D: Use parts (B) and (C) to show that a Fermat number \( F_n = 2^{2^n} + 1 \) is prime if and only if \( 5^{F_n-1} \equiv -1 \pmod{F_n} \).
E: Suppose \( M_\ell = 2^n - 1 \) is (a Mersenne) prime. Show that 2 is a square \( \pmod{M_\ell} \), but 3 is \textbf{not} a square \( \pmod{M_\ell} \). Use these facts to show that the system of equations:

\[
\begin{align*}
x^2 + 3y^2 &= 2 \\
x^2 - 3y^2 &= 1
\end{align*}
\]

does not have a solution.

\textbf{Hint:} Add the two equations.

Problems for Friday: \( p \) is an odd prime.

1: Let \( G \) be a finite cyclic group; write \( \zeta \) for a generator so that
\( G = \{\zeta, \zeta^2, \ldots, \zeta^{d-1} \neq e, \zeta^d = e\} \). Show that any subgroup \( H \subset G \) must be cyclic as well. Show that an element \( a \in G \) is of the form \( a = b^2 \) if and only if \( a = \zeta^{2k} \) for some \( k \in \mathbb{N} \).

\textbf{Hint:} Let \( a > 0 \) be the smallest integer so that \( \zeta^a \in H \). Since \( G \) is cyclic, any other element of \( H \) is of the form \( \zeta^b \). Show that \( a \mid b \).

2: Let \( R = \mathbb{Z}_p[\sqrt{d}] = \{a + b\sqrt{d} : a, b \in \mathbb{Z}_p\} \). In a previous exercise you showed that if \( d \) is not a square in \( \mathbb{Z}_p \), then \( R \) is a field. Let \( G = \mathbb{Z}_p[\sqrt{d}]^\times \). You also showed that \( G \) has \( p^2 - 1 \) elements. Adapt the proof that \( \mathbb{Z}_p^\times \) is a cyclic group to show that \( \mathbb{Z}_p[\sqrt{d}]^\times \) is cyclic.

3: Define \( N(a + b\sqrt{d}) := (a + b\sqrt{d})(a - b\sqrt{d}) = a^2 - b^2d. \) Show that \( N(\alpha \cdot \beta) = N(\alpha)N(\beta), \) and that \( T_p := \{\alpha = a + b\sqrt{d} : N(\alpha) = 1\} \) is a subgroup of \( G \).

4: Let \( \zeta = a + b\sqrt{d} \) be a generator (primitive root) of \( G \). Show that \( \zeta^p = a - b\sqrt{d}, \) (called the conjugate of \( \alpha \), denoted \( \overline{\alpha} \)). Use this to show that \( T_p \) is cyclic of order \( p + 1 \), generated by \( \zeta^{p-1} \).

5: Show that an element \( a \in T_p \) is a square (i.e. \( a = b^2 \) for \( b \in T_p \)) if and only if \( a^{p+1} = +1 \).

6: Assume \( M_\ell = 2^\ell - 1 \) is prime. Show that \( 2 + \sqrt{3} \in T_{M_\ell} \), but cannot be the square of an element in \( T_{M_\ell} \) (use problem E). In particular, since \( M_\ell + 1 = 2^\ell \), show that the order of \( 2 + \sqrt{3} \) must be \( 2^\ell \), and in particular \( (2 + \sqrt{3})^{2^\ell - 1} = -1 \pmod{M_\ell} \).

7: Assume \( (2 + \sqrt{3})^{2^\ell - 1} = -1 \). Explain why \( M_\ell \) must be a prime.

\textbf{Hint:} If \( M_\ell \) is not prime, there is a prime \( 2 < p < \sqrt{M_\ell} \). Recall that \( 2 + \sqrt{3} \in \mathbb{Z}_p[\sqrt{d}]^\times \), so its order must be smaller than \( p^2 - 1 \).