Homework 10 : Due Wednesday, May 2

Problem 1: Let $a \in \mathbb{Z}$ be odd and let $k \in \mathbb{N}$ with $k \geq 3$. Prove that a is a quadratic residue modulo 2^k if and only if $a \equiv 1 \pmod{8}$.
Note: This is the last result that allows us to reduce questions about quadratic residues modulo n to quadratic residues modulo primes.

Problem 2: Consider the polynomial $f(x) = x^6 + x^4 - 4x^2 - 4 \in \mathbb{Z}[x]$. Show that $f(x)$ has a root modulo every prime $p \in \mathbb{N}^+$, but $f(x)$ has no integer roots.
Hint: Begin by factoring $f(x) = (x^2 + 1)(x^4 - 4)$.

Problem 3: Suppose that $p \in \mathbb{N}^+$ is a prime with $p \equiv 1 \pmod{3}$.
a. Using the tools from class, show that -3 is a quadratic residue modulo p.
b. Here we give a more constructive proof of a without using Quadratic Reciprocity. Since $p \equiv 1 \pmod{3}$, the group $U(\mathbb{Z}/p\mathbb{Z})$, having $p-1$ elements, has order divisible by 3. Since $U(\mathbb{Z}/p\mathbb{Z})$ is a cyclic group with order some multiple of 3, there exists $b \in \mathbb{Z}$ such that $\overline{b} \in U(\mathbb{Z}/p\mathbb{Z})$ has order 3. Show that $(2b+1)^2 \equiv -3 \pmod{p}$.

Problem 4: Suppose that $d \in \mathbb{N}^+$ is square-free and that d has a prime divisor p with $p \equiv 3 \pmod{4}$. Show that every element of $U(\mathcal{O}_{\mathbb{Q}(\sqrt{d})})$ has norm 1.

Problem 5: Let $R = \mathcal{O}_{\mathbb{Q}(\sqrt{-5})}$. We know that R is not a PID and in fact you showed on Homework 8 that $\langle 2, 1 + \sqrt{-5} \rangle$ is nonprincipal. Thus, there is no guarantee that greatest common divisors always exist in R.
a. Show that 2 and $1 + \sqrt{-5}$ do in fact have a greatest common divisor in R.
b. Show that if $\delta \in R$ is a greatest common divisor of 2 and $1 + \sqrt{-5}$, then there do not exist $\alpha, \beta \in R$ with $\delta = 2\alpha + (1 + \sqrt{-5})\beta$.
c. Show that 6 and $2 + 2\sqrt{-5}$ do not have a greatest common divisor in R.

Problem 6: Let $p \in \mathbb{N}^+$ be an odd prime. We defined

$$G = \sum_{k=0}^{p-1} \left(\frac{k}{p}\right) \zeta_p^k$$

Show that

$$G = \sum_{k=0}^{p-1} \zeta_p^{k^2}$$