

MATH 4400
HOMEWORK 5
DUE 2/28/08

Instructions: Math 6400 students should do all the problems. Math 4400 students should do five of the seven problems.

Problem 1: A prime p is called a *Sophie Germain prime* if $2p + 1$ is also prime. In this case, $2p + 1$ is sometimes called the *safe prime*. Show that if $p > 3$ is a Sophie Germain prime congruent to $3 \pmod{4}$, then $2^p - 1$ is composite. (Hint: What is $2^p \pmod{2p + 1}$?)

Problem 2: Let p be an odd prime. This exercise outlines a proof that $\mathbb{Q}(\zeta_p)$ contains $\mathbb{Q}(\sqrt{p^*})$, where $p^* = \left(\frac{-1}{p}\right)p$. For the rest of the problem, let $f_p(x) = x^p - 1$ and let $\zeta = \zeta_p$.

(a) Fix i such that $0 \leq i \leq p - 1$. Show that

$$f'_p(\zeta^i) = \prod_{j \neq i} (\zeta^i - \zeta^j).$$

(Here j runs over $\{0, \dots, p - 1\}$ but skips i .)

(b) By part (a), we get

$$\prod_{i=0}^{p-1} f'_p(\zeta^i) = \prod_{i=0}^{p-1} \prod_{j \neq i} (\zeta^i - \zeta^j).$$

Show that the left side equals p^p .

(c) Now show that the right side equals

$$\left(\frac{-1}{p}\right) \prod_{i < j} (\zeta^i - \zeta^j)^2$$

where the product runs over all ordered pairs (i, j) with $0 \leq i < j \leq p - 1$. (Hint: how many terms of the right side of part (b) have to get flipped?)

(d) Conclude that $\sqrt{p^*} \in \mathbb{Q}(\zeta_p)$.

Remark: In fact, one can show that $\mathbb{Q}(\sqrt{p^*})$ is the *unique* quadratic subfield of $\mathbb{Q}(\zeta_p)$. This fact is important in some proofs of quadratic reciprocity.

Problem 3: Let n be an odd positive integer. Show that

$$\left(\frac{2}{n}\right) = (-1)^{\frac{n^2-1}{8}}.$$

Problem 4: Show that

$$\sum_{n \leq x} \sigma_0(n) = x \ln x + O(x).$$

Problem 5: (a) Show that $\mathbb{Z}[\sqrt{2}]$ and $\mathbb{Z}[\sqrt{3}]$ are PIDs.

(b) Show that $\mathbb{Z}[\sqrt{-3}]$ and $\mathbb{Z}[\sqrt{5}]$ are not PIDs.

Problem 6: (a) Find, with proof, a description of all primes p that can be written as $x^2 - 2y^2$, where $x, y \in \mathbb{Z}$.

(b) Do the same for $x^2 - 3y^2$. (Warning for both problems: careful when you run the standard argument, as norms of elements of $\mathbb{Z}[\sqrt{d}]$ might be negative!)

Problem 7: For any nonconstant polynomial $f(x) \in \mathbb{Z}[x]$, show that there are infinitely many primes p such that $f(x)$ has a root in \mathbb{F}_p .

Remark: We used this argument in the special case $f = \Phi_n$ to show that there were infinitely many primes congruent to 1 mod n .