

MATH 4400
HOMEWORK 8
DUE 4/22/08

Instructions: 4400 students should do problems 1, 2, 3, and 6. You should try problem 4 as well. Do as much as you can. 6400 students should do everything.

Problem 1: Consider the binary quadratic forms $Q_1(x, y) = x^2 + 9y^2$ and $Q_2(x, y) = x^2 + 12y^2$.

(a) Show that any prime p represented by Q_1 is congruent to 1 mod 12. Show that the same is true for Q_2 .

(b) Show that Q_1 represents *all* primes congruent to 1 mod 12. (Hint: you know which ones $x^2 + z^2$ represents; show that if $p = x^2 + z^2$ and $p \equiv 1 \pmod{12}$, then either x or z is divisible by 3.)

(c) Show that Q_2 represents exactly the same primes as Q_1 does. (Hint: similar hint to the last problem, except start with the quadratic form $x^2 + 3z^2$.)

Remark: A recent talk in the number theory seminar classified all pairs of quadratic forms which represent “almost” the same primes; this was the first example.

Problem 2: As usual, let F be a field of characteristic $\neq 2$. Show that every quadratic form over F is equivalent to a diagonal one. (Hint: this should be pretty easy if you remember the *Gram-Schmidt* process, I think. Or you can try induction and the down-to-earth changes of variables I’ve been hinting at in class...)

Problem 3: Let d be a squarefree integer. Let $\tau_d = \frac{1 + \sqrt{d}}{2}$. As in class, we define an *algebraic integer* to be a complex number which is a root of a monic polynomial in $\mathbb{Z}[x]$. Let \mathcal{O}_d be the set of algebraic integers inside $\mathbb{Q}(\sqrt{d})$. Show that

$$\mathcal{O}_d = \begin{cases} \mathbb{Z}[\sqrt{d}] & \text{if } d \equiv 2 \text{ or } 3 \pmod{4} \\ \mathbb{Z}[\tau_d] & \text{if } d \equiv 1 \pmod{4} \end{cases}$$

Problem 4: Let a and b be two nonzero rational numbers, and let p be a prime. Define the *Hilbert symbol* $(a, b)_p$ as follows:

$$(a, b)_p = \begin{cases} 1 & \text{if } x^2 - ay^2 - bz^2 \text{ is isotropic over } \mathbb{Q}_p \\ -1 & \text{otherwise} \end{cases}$$

(a) Suppose a and b are not squares in \mathbb{Q}_p (if one of them is, then of course $(a, b)_p = 1$). Show that the following three statements are equivalent:

- (1) $(a, b)_p = 1$
- (2) b is the norm of some element in $\mathbb{Q}_p(\sqrt{a})$
- (3) a is the norm of some element in $\mathbb{Q}_p(\sqrt{b})$

(Hint: careful! how do you know y or z isn't zero?)

(b) Show that $x^2 - ay^2 - bz^2 = 0$ has a nontrivial solution mod p if $|2ab|_p = 1$. (It's ok to reduce the rational numbers a and b mod p , because the condition guarantees that there aren't any p 's in the denominator.)

(c) Use Hensel's lemma to deduce that $(a, b)_p = 1$ if $|2ab|_p = 1$. Conclude that $(a, b)_p = 1$ for all but finitely many p .

Problem 5: This problem concerns a more general form of Hensel's lemma.

(a) Suppose $f(x)$ is a polynomial in $\mathbb{Z}_p[x]$. Suppose that $|f(\alpha)|_p < |f'(\alpha)|_p^2$. Show that there exists $\beta \in \mathbb{Z}_p[x]$ such that $f(\beta) = 0$, and $|\alpha - \beta|_p < 1$.

(b) Why is this a generalization of the original Hensel's lemma we proved in class?

(c) Show that the squares in \mathbb{Q}_2^* are precisely the elements of the form $4^k(1 + 8t)$, where $t \in \mathbb{Z}_p^*$.

Problem 6: Consider the equation $x^2 + 17y^2 = 257$.

(a) Show that this equation has no integer solutions.

(b) Show that this equation has nontrivial solutions in \mathbb{R} and in \mathbb{Z}_p for $p \neq 2, 17$, or 257 . (The argument is the same as that in 4(b) and (c); use Hensel's lemma.)

(c) Also show that the equation has nontrivial solutions in \mathbb{Z}_{17} and \mathbb{Z}_{257} . Finally, use problem 5 to show that it has nontrivial solutions in \mathbb{Z}_2 .