MATH 124 HOMEWORK #6

INNA ZAKHAREVICH

(1) We know that a number can be expressed as the sum of two squares if and only if all prime factors of the form $4k+3$ appear to an even power. Factoring, we get the following table:

Number	Factorization	Expression
97	97	9^2+4^2
221	$13\cdot 17$	$(3^2+2^2)(4^2+1^2)=10^2+11^2$
300	$2^2\cdot \underline{3}\cdot 5^2$	N/A
490	$2\cdot 5\cdot 7^2$	$(7^2+0^2)(3^2+1^2)=21^2+7^2$
729	3^6	27^2+0^2
1001	$7\cdot \underline{11}\cdot 13$	N/A
490490	$2\cdot 5\cdot 7^3\cdot \underline{11}\cdot 13$	N/A

(2) We know that $67^2\equiv -1 \pmod{449}$. Thus we take the continued fraction expansion of $449/67$, which is

$$\langle 6,1,2,2,1,6\rangle.$$

This is symmetric with $m=3$.

(3) (a) We compute

$$\left(\frac{-5}{23}\right)=\left(\frac{-1}{23}\right)\left(\frac{5}{23}\right)=-\left(\frac{23}{5}\right)=-\left(\frac{3}{5}\right)=1$$

so the equation $h^2\equiv -5 \pmod{23}$ has a solution.

(b) Consider the given equation modulo 5. We have that $x^2\equiv 23 \pmod 5$, which is impossible since 3 is not a square modulo 5.

(c) We want to show that there are two nonequivalent quadratic forms of discriminant -5. Suppose that all quadratic forms of discriminant -5 were equivalent. Then the fact that there is a solution to the equation in part (a) would mean that there is a solution to $x^2+5y^2=23$. However, this is not the case; constradiction. Thus there must be at least two nonequivalent quadratic forms of discriminant -5.

(4) (a) We will show that there is exactly one reduced form not equal to $(1,0,3)$ with discriminant -12, and thus we will know that there are exactly two equivalence classes for forms with discriminant -12. We will also compute in the course of this proof what the form must equal.

Suppose that we have a reduced quadratic form of discriminant -12. Note, first, that any such form must have even b, since we have $b^2=-12+4ac$. Suppose that $b\neq 0$, since then we must have the form equivalent to $(1,0,3)$. Thus we can write the form as

$$ax^2+2bxy+cy^2.$$

Since the form is reduced we know that $|2b| \leq a \leq c$. But because the form has discriminant -12 we also know that $b^2 = ac - 3$. Suppose that $|2b| < a$, so $|b| < a - |b| \leq a - 1$ (since $b \neq 0$). Also, since $2 < |2b| < a$ we get $1 - 2a < -3$. Then we know

$$b^2 < (a-1)^2 = a^2 - 2a + 1 < a^2 - 3 \leq ac - 3 = b^2,$$

a contradiction. Thus we must have $|2b| = a$; writing $a = 2a_0$ we get that $b^2 = 2a_0c - 3$ and $a_0^2 = b^2$. Thus we have $a_0^2 - (2c)a_0^2 + 3 = 0$. Thus must have integer roots, so we must have $c = \pm 2$ and $a_0|3$. Since $|b| \leq a \leq c$ we need $c = 2, a_0 = 1, b = \pm 1$. thus we get the forms

$$2x^2 \pm 2xy + 2y^2,$$

which are equivalent. Thus the two different forms with discriminant -12 are

$$x^2 + 3y^2 \qquad 2x^2 + 2xy + 2y^2.$$

(b) First suppose that $p > 3$. Consider the quadratic form

$$px^2 + \alpha xy + \beta y^2$$

which represents p. We want to show that this is equivalent to $x^2 + 3y^2$ if and only if $p \equiv 1 \pmod 6$. First, notice that this form has discriminant -12 is and only if $p \equiv 1 \pmod 6$, since we must have

$$4p\beta - \alpha^2 = 12,$$

which means that $\left(\frac{-12}{p}\right) = \left(\frac{-3}{=}\right) 1$ which happens if and only if $p \equiv 1 \pmod 6$ (as in a previous problem set). Thus we know that we have a quadratic form of discriminant -12 with p as the first coefficient (so we have a quadratic form of discriminant -12 representing p) if and only if $p \equiv 1 \pmod 6$. Thus if $p \not\equiv 1 \pmod 6$ it must not be representable by the form $x^2 + 3y^2$.
So now we want to show that if

$$px^2 + \alpha xy + \frac{12 + \alpha^2}{4p} y^2$$

is a quadratic form then it is equivalent to $x^2 + 3y^2$. Note from the above form that $\alpha^2 \equiv 0 \pmod 4$, so α must be even. Thus we can write $\alpha = 2\gamma$, and the form looks like

$$px^2 + 2\gamma xy + \frac{3 + \gamma^2}{p} y^2.$$

Note that the first coefficient of this form is odd. Any transformation of the quadratic form $2x^2 + 2xy + 2y^2$ will have all coefficients even, which means that the above form is not equivalent to this. Thus we know that this form is equivalent to $x^2 + 3y^2$, so we have shown that if $p \equiv 1 \pmod 6$ then it is representable by the form $x^2 + 3y^2$.
Lastly we consider the cases $p = 2, 3$. Clearly, 2 is not represented by $x^2 + 3y^2$ but 3 is. Thus we have shown that p is representable as $x^2 + 3y^2$ if and only if $p = 3$ or $p \equiv 1 \pmod 6$.