DUE DATE: FEB. 28, 2008

1. There is a rather surprising formula which counts the number of ways that a positive integer n can be written as a sum of two squares:

$$(*) \qquad \#\left\{(x,y)\in\mathbb{Z}^2 \mid x^2+y^2=n\right\} = 4\sum_{\substack{d|n\\ d\,\text{odd}}}(-1)^{\frac{d-1}{2}}$$

The proof of this formula is slightly beyond the methods of this class, but let's at least try it out in some examples, and see that it implies parts of the theorem that we proved.

To make the notation slightly easier set $f(n) = 4\sum_{\substack{d|n\\ d\,\text{odd}}}(-1)^{\frac{d-1}{2}}$.

(a) For $n = 221 = 13\cdot 17$ compute $f(n)$ and list all the ways to write n as a sum of two squares as above.

(b) Do the same thing for $n = 31117 = 29^2\cdot 37$.

HINT: Don't forget that there is a product formula for writing a number as a sum of squares: If you know how to write n_1 and n_2 as a sum of squares then this gives you an explicit expression for $n = n_1n_2$ as a sum of two squares.

NOTE: Since order matters (if (x,y) is a solution then (y,x) is a solution), and so do signs (i.e., $(\pm x, \pm y)$ are solutions), in describing the solutions to $x^2+y^2=n$ it's enough to list the solutions with x, $y\geq 0$ and $x\geq y$, and then say how many other solutions are generated from each pair by the process of switching the order and switching the signs.

(c) If d is an odd number, show that $(-1)^{\frac{d-1}{2}} = \begin{cases} 1 & \text{if } d\equiv 1 \pmod 4 \\ -1 & \text{if } d\equiv 3 \pmod 4\end{cases}$

(d) Give a formula in terms of e for $f(p^e)$ where p is an odd prime and e a positive integer. (Your answer may depend on whether $p\equiv 1$ or $3 \pmod 4$.)

(e) If formula (*) is really true (that is, if $f(n)$ really counts the number of ways to write n as a sum of two squares) show that this would imply that every prime number $p\equiv 1 \pmod 4$ is the sum of two squares, and that no prime number $p\equiv 3 \pmod 4$ is the sum of two squares.

2. In this problem we want to try and understand the "sums of two squares" problem for polynomials over $\mathbb{R}$. The question is: When can a polynomial $n(x) \in \mathbb{R}[x]$ be written as the sum of two squares, $n(x) = (f(x))^2 + (g(x))^2$, with $f(x)$, $g(x) \in \mathbb{R}[x]$?

We will use one fact not proved in this class: Every polynomial $n(x)$ in $\mathbb{R}[x]$ can be factored uniquely into a product of linear factors and irreducible quadratic factors. That is, every polynomial $n(x) \in \mathbb{R}[x]$ can be factored uniquely as:

$$n(x) = \kappa(x-a_1)^{e_1}(x-a_2)^{e_2}\cdots(x-a_k)^{e_k}(x^2+b_1x+c_1)^{f_1}(x^2+b_2x+c_2)^{f_2}\cdots(x^2+b_\ell x+c_\ell)^{f_\ell}$$

Where the numbers a_i, b_j, c_k, and κ are in $\mathbb{R}$, and "irreducible quadratic" means that $b_k^2 - 4c_k < 0$ for $k = 1, \ldots, \ell$, i.e., these quadratic polynomials have no real roots.

(More precisely, we will prove unique factorization in class, but the fact that the prime polynomials in $\mathbb{R}[x]$ are linear terms and quadratics is a consequence of the "fundamental theorem of algebra", which we will not prove).

(a) If $n(x) \in \mathbb{R}[x]$ is a sum of squares, explain why $n(x) \geq 0$ for all $x \in \mathbb{R}$.

(b) If one of the linear factors in the factorization of $n(x)$ has an odd exponent (i.e., one of the numbers e_i above is odd) explain why $n(x)$ must change sign at some point, and therefore why $n(x)$ cannot be a sum of squares.

(c) Show that any positive real number κ can be written as a sum of two squares.

(d) Show that for any $a \in \mathbb{R}$, $(x-a)^2$ can be written as a sum of two squares.

(e) If $x^2 + bx + c$ is an irreducible quadratic polynomial (i.e., $b^2 - 4c < 0$) show that it can be written as a sum of squares. (HINT: Complete the square).

(f) Which polynomials in $\mathbb{R}[x]$ can be written as a sum of two squares? Formulate the correct theorem and use (a)–(e) above to prove it.

3. Suppose that R is a domain and that $a(x)$ and $b(x)$ are two elements of $R[x]$ such that $a(x) \mid b(x)$ and $b(x) \mid a(x)$. Show that there is a unit u in $R[x]$ so that $b(x) = ua(x)$. If the leading coefficients of $a(x)$ and $b(x)$ are the same, show that this implies that $b(x) = a(x)$.