MATH 342 Problem Sheet 11: sums of squares

Due Tuesday 7th May

1.

a) Show that if $p > 7$ is prime then

$$\left(\frac{-7}{p}\right) = 1 \Leftrightarrow p \equiv 1 \bmod 7 \vee p \equiv 2 \bmod 7 \vee p \equiv 4 \bmod 7.$$

b) Show that if $p > 7$ is prime and $p = a^2 + 7b^2$ for integers a and b then p is congruent to 1, 2 or 4 mod 7.

c) Deduce from a) that if p is congruent to 1, 2 or 4 mod 7, then there is an integer c such that $c^2 + 7$ is divisible by p.

2. List all the odd primes less than 100 which are congruent to 1, 2 or 4 mod 7. For each such prime p, find integers a and b such that $p = a^2 + 7b^2$.

3. Show that if c and d are both odd integers then $(c/2)^2 + 7(d/2)^2$ is an even integer. You may use the fact that both c^2 and d^2 are congruent to $1 \bmod 8$. Use this to show that the square of the modulus $|z|^2$ is an integer for any $z \in \mathcal{O}[\sqrt{-7}]$ where

$$\mathcal{O}[\sqrt{-7}] = \{a+b\sqrt{-7} : a+b \in \mathbb{Z} \wedge a-b \in \mathbb{Z}\} = \{a+b\sqrt{-7} : (a \in \mathbb{Z} \wedge b \in \mathbb{Z}) \vee (a+\frac{1}{2} \in \mathbb{Z} \wedge b+\frac{1}{2} \in \mathbb{Z})\}$$

(You may assume that these two different descriptions of $\mathcal{O}[\sqrt{-7}]$ are equivalent.)

4. You may assume that $\mathcal{O}[\sqrt{-7}]$ is a Euclidean domain with Euclidean valuation $v(z) = |z|^2$, and hence a unique factorisation domain.

Show that if $a + b\sqrt{-7} \in \mathcal{O}[\sqrt{-7}]$ divides an integer m in $\mathcal{O}[\sqrt{-7}]$, then $a - b\sqrt{-7}$ also divides m in $\mathcal{O}[\sqrt{-7}]$. Deduce that if $a + b\sqrt{-7}$ is prime in $\mathcal{O}[\sqrt{-7}]$ and both a and b are non-zero, then $a^2 + 7b^2$ divides m in $\mathbb{Z}$.

Hint: In a unique factorisation domain $\mathcal{O}$, if two inequivalent primes $x_1 \in \mathcal{O}$ and $x_2 \in \mathcal{O}$ both divide $x \in \mathcal{O}$, then x_1x_2 also divides x in $\mathcal{O}$. Primes x_1 and x_2 are said to be *inequivalent* if $x_2 \neq x_1u$ for any unit $u \in \mathcal{O}$. The only units in $\mathcal{O}[\sqrt{-7}]$ are ± 1.

5. Once again, you may assume that $\mathcal{O}[\sqrt{-7}]$ is a unique factorisation domain. Let p be any odd prime which is congruent to 1, 2 or 4 mod 7 Use the fact that $np = c^2 + 7$ for some integers c and n to deduce the existence of integers a and b such that $p = a^2 + 7b^2$.

Hint: You may use the fact some prime $z = a + b\sqrt{-7}$ (where a and b are half integers) in $\mathcal{O}[\sqrt{-7}]$ which divides $c + \sqrt{-7}$ must divide p. (This uses unique factorisation of np in $\mathcal{O}[\sqrt{-7}]$.) Then use question 4. Use question 3 to deduce that a and b are integers, not just half integers.

I will collect solutions at the lecture on Tuesday 7th May. Any solutions which are not handed in then, or by 5pm that day in the folder outside room 516 will not be marked.