MATH 342 Problem Sheet 9: Pythagorean triples and quadratic number fields

Due Monday 22nd April

1.

a) Prove that if x and y are any two integers which are both even or both odd then there are integers p and q such that $xy = p^2 - q^2$.

b) Prove that if n is an integer which is $2 \mod 4$ then n cannot be written in the form $p^2 - q^2$ for integers p and q.

2. A *Pythagorean triple* is a triple (x, y, z) of strictly positive integers such that $x^2 + y^2 = z^2$.

a) Prove that it is impossible for both x and y to be odd.

b) Prove that it is impossible to have $x = y$.

3. If x and y are even, then of course z is too, and $(x/2, y/2, z/2)$ is also a Pythagorean triple. For this question we assume that (x, y, z) is a Pythagorean triple in which x is odd, so that y is even and z is odd. For similar reasons, we assume that p and q are coprime. The theory of Pythagorean triples then tells us that there are nonzero integers p and q such that

$$x + iy = (p + iq)^2, \quad z = |p + iq|^2 = p^2 + q^2.$$

If x is odd then one of p and q must be even and the other is odd. Otherwise all possibilities occur. Write down the Pythagorean triples for such p and q, where $1 \leq q < p \leq 8$.

4. Identify for which of these $p^2 + q^2$ is *not* prime. You will see two different rows of the table for one of these – and there would be two different rows for another, if the table were continued. Explain this.
Hint: If $|p + qi|^2$ is odd $|p + qi|^2 = |(p + qi)^2| = |(p_1 + iq_1)^2(p_2 + q_2 i)^2|$ where $p_1 + q_1 i$ and $p_2 + q_2 i$ are distinct primes in $\mathbb{Z}[i]$ and all of p_1, q_1, p_2 and q_2 are non-zero, then there are two choices for $p + qi$ with p and q coprime which are distinct, even after multiplying by ± 1 or $\pm i$. Can you see why?

5. As on Sheet 8, define

$$\mathcal{O}[\sqrt{5}] = \{c_1 + c_2\sqrt{5} : c_1 + c_2 \in \mathbb{Z} \wedge c_1 - c_2 \in \mathbb{Z}\}.$$

This ring properly contains $\mathbb{Z}[\sqrt{5}]$. You were asked to prove on Sheet 8 that v maps $\mathcal{O}[\sqrt{5}]$ into $\mathbb{N}$ where, for $c_1 + c_2 \in \mathbb{Z} \wedge c_1 - c_2 \in \mathbb{Z}$,

$$v(c_1 + c_2\sqrt{5}) = |c_1^2 - 5c_2^2|$$

You may therefore assume this. You may also assume that v is multiplicative, that is, $v(cd) = v(c)v(d)$. On Sheet 8 you were asked to prove that $c_1 + c_2\sqrt{5} \in \mathcal{O}[\sqrt{5}]$ is a unit in $\mathcal{O}[\sqrt{5}]$ if and only if

$$v(c_1 + c_2\sqrt{5}) = c_1^2 - 5c_2^2 = \pm 1.$$

The same proof works for units in $\mathbb{Z}[\sqrt{5}]$. You may assume both of these.

a) Prove that there are no integers a and b such that $a^2 - 5b^2 \equiv 2 \mod 4$. Prove also that if a and b are both odd integers then $a^2 - 5b^2 \equiv 4 \mod 8$. You may assume that if a is an odd integer then $a^2 \equiv 1 \mod 8$.

b) Prove that 2 is irreducible in $\mathbb{Z}[\sqrt{5}]$ and in $\mathcal{O}[\sqrt{5}]$.

Hint Why is it enough to show that there are no integers a and b with $a^2 - 5b^2 = \pm 2$, and no odd integers a and b with $a^2 - 5b^2 = \pm 8$?

c) Find a and $b \in \mathbb{Z}$ such that $a^2 - 5b^2 = \pm 4$. Explain why this gives two essentially factorisations of 4 into irreducibles in $\mathbb{Z}[\sqrt{5}]$, but not in $\mathcal{O}[\sqrt{5}]$.

I will collect solutions at the lecture on Monday 22nd April. Any solutions which are not handed in then, or by 5pm that day in the folder outside room 516 will not be marked.