**MATH3320 HW3 (Solution)**

Outline of methods and remarks

**Q1** Since all the factors of 15 are 1, 3, 5 and 15, we have to solve for each one for \(a\) and \(b\) where \((x, y, z) = (a^2 - b^2, 2ab, a^2 + b^2)\) for possible values of \(x\), \(y\) and \(z\).

For 1, there is no good values of \(a\) and \(b\) that gives \(x = 1\), \(y = 1\) or \(z = 1\).

For 3, the only possibility is \(a = 2\) and \(b = 1\) which gives \((x, y, z) = (3, 4, 5)\) and hence the triple \((15, 20, 25)\) that we are looking for.

For 5, the only possibilities are \((x, y, z) = (3, 4, 5)\) and \((5, 12, 13)\) which gives the triples \((9, 12, 15)\) and \((15, 36, 39)\).

Finally for 15, we see that \(15 = 2ab\) has no solutions in \(a\) and \(b\) since 15 is odd. Also, \(15 = a^2 + b^2\) has no solutions because \(15 \equiv 3 \pmod{4}\). Therefore we are left to solving \(a^2 - b^2 = 15\) which has two solutions \((a, b) = (8, 7)\) and \((4, 1)\) and the corresponding triples are \((15, 112, 113)\) and \((15, 8, 17)\).

**Q5** Can be done either by brute force, or by the fact that \(77 = 7 \cdot 11\); neither 7 nor 11 are of the form \(4k + 1\), so they are prime in \(\mathbb{Z}[i]\); they cannot be written as \(a^2 + b^2\). So \(77^2 = 7^2 \cdot 11^2\) cannot be written as a sum of squares either.

**A** Suppose \(\bar{a} = \bar{\beta} \cdot \bar{\gamma}\), then \(a = \beta \cdot \gamma\). Since \(a\) is a unit, one of \(\bar{\beta}\) or \(\bar{\gamma}\) is a unit. Therefore one of \(\beta\) or \(\gamma\) is a unit. Since this is true for all factorizations \(\bar{a} = \beta \cdot \gamma\), we conclude that \(a\) is a prime.

(Since \(\bar{a} = a\), by symmetry we have the stronger statement that \(a\) is prime if and only if \(\bar{a}\) is prime.)

(Note that for example “\(\beta\) is a unit” is the same as saying “\(N(\beta) = 1\)”.)

**B** Because \(\gcd(9 + 7i, 13) = 2 + 3i\) is not an integer, and 13 is a prime in \(\mathbb{Z}\), \(2 \pm 3i\) are prime in \(\mathbb{Z}[i]\), and so 13 necessarily equals \((3+2i)(3-2i) = 3^2 + 2^2\), a sum of squares. In general \(\gcd(\alpha, \beta) = \gamma\) does not give an expression for \(\alpha\) or \(\beta\) as a sum of squares. Problem D is the more usual situation, we know \(9^2 + 7^2 = 130 = 13 \cdot 2 \cdot 5\), and we can use the \(\gcd\) to express 2, 5, 13 as sums of squares.

**C** \(\pi|N\) hence \(\bar{\pi}|\bar{N} = N\) (as \(N\) is real). By A we know that \(\bar{\pi}\) is also prime, so \((\pi, \bar{\pi}) = 1\) or \(\pi\).

In the case \((\pi, \bar{\pi}) = 1\), \(\pi|N\) and \(\bar{\pi}|N\) implies \(\pi \cdot \bar{\pi}|N\).
In the case \((\pi, \bar{\pi}) = \pi, \pi|\bar{\pi}\) means \(\pi\) and \(\bar{\pi}\) are conjugates. That is, either \(\bar{\pi} = i\pi\) or \(\bar{\pi} = \pi\). That is, \(a - bi = -b + ai\) or \(b = 0\). In the first case, since \(\pi\) is prime, we have \(a = b = 1\) and it can be checked that \(1 + i|N\) implies \(2|N\) (by taking norm on both sides and consider factorization over \(\mathbb{Z}\)). This is exactly what we want because \((1 + i)(1 - i) = 2\). In the second case we must have \(\pi = p\) where \(p\) is a rational prime in the form \(4k + 3\). And this is where the claim fails: for example \(7|14\) but \(7 \cdot \bar{7} = 49 \not| 14\).

Therefore the question should be modified with an additional assumption: “assume that both \(a\) and \(b\) are nonzero”.

D This is basically the idea behind the proof of Fermat’s theorem that any rational prime of the form \(4k + 1\) can be expressed as a sum of two squares.