MATH342 Feedback and Solutions 9

1.

a) Since $p^2 - q^2 = (p+q)(p-q)$, we look for p and q with

$$x = p + q, \quad y = p - q,$$

that is,

$$p = \frac{x+y}{2}, \quad q = \frac{x-y}{2}.$$

If x and y are both even or both odd, then $x+y$ and $x-y$ are both even, and hence p and q are both integers.

This question asked to show that if x *and* y *are both odd or both even* then p *and* q *are integers – not the converse, which is what some solutions that I saw did. The converse is also true of course.*

b) Since $p + q = p - q + 2q$, either both $p+q$ and $p-q$ are odd or they are both even. If they are both odd then $(p-q)(p+q)$ is odd and if they are both even then $(p-q)(p+q) \equiv 0 \mod 4$.

An alternative solution that I saw, also correct, used that each of p^2 *and* q^2 *is either* $0 \mod 4$ *or* $1 \mod 4$. *That gives* 4 *choices for* $(p \mod 4,\ q \mod 4)$, *of which two give* $p^2 - q^2 = 0 \mod 4$ *and the other two give* $\pm 1 \mod 4$. *So* $2 \mod 4$ *is not possible.*

2.

a) If x and y are both odd then $x^2 \equiv 1 \mod 4$ and $y^2 \equiv 1 \mod 4$ and so

$$z^2 = x^2 + y^2 \equiv 2 \mod 4.$$

So z is even. But then $4 \mid z^2$ and $z^2 \equiv 0 \mod 4$, which is a contradiction.

b) If $x = y$, then $x^2 + y^2 = 2x^2$, and $z^2 = 2x^2$ is divisible by an odd power of 2. But the maximal power of any prime dividing z^2 is even.

This is essentially the proof that $\sqrt{2}$ *is irrational, because* $z^2 = 2x^2$ *for strictly positive integers* z *and* x *if and only if* $\sqrt{2} = x/z$ *for strictly positive integers* x *and* z, *that is, if and only if* $\sqrt{2}$ *is rational. The notation for the set of rational numbers is* $\mathbb{Q}$, *not* $\mathbb{Z}$.

3. The table is as follows, ordered in increasing values of $p^2 + q^2$.

$p + qi$	$p^2 - q^2$	$2pq$	$p^2 + q^2$
$2 + i$	3	4	5
$3 + 2i$	5	12	13
$4 + i$	15	8	17
$4 + 3i$	7	24	25
$5 + 2i$	21	20	29
$6 + i$	35	12	37
$5 + 4i$	9	40	41
$7 + 2i$	45	28	53
$6 + 5i$	11	60	61
$8 + i$	63	16	65
$7 + 4i$	33	56	65
$8 + 3i$	55	48	73
$7 + 6i$	13	84	85
$8 + 5i$	39	80	89
$8 + 7i$	15	112	113

Some did not notice that it is only necessary to consider (p, q) *such that exactly one of* p *and* q *is even. The question did specify this. If both* p *and* q *are odd or both even, then all three of the numbers* $(p^2 - q^2, 2pq, p^2 + q^2)$ *in the Pythagorean triple are even.*

4. The non-prime values of p^2+q^2 are $25 = 5\times 5$, $65 = 5\times 13$ and $85 = 5\times 17$.

The three primes 5, 13 and 17 occur earlier in the table. There are two rows with $p^2+q^2 = 65$, and there would be two with $p^2+q^2 = 85$, if the table were continued. The reason is that, if p^2+q^2 is not a prime integer, then$(p+qi)(p-qi) = n_1n_2$ for integers $n_1 > 1$ and $n_2 > 1$. But then by unique factorisation of $\mathbb{Z}[i]$, it cannot be the case that both $p+qi$ and $p-qi$ are prime. Since complex conjugation preserves multiplication, they are both not prime. So there are p_1, q_1, p_2 and $q_2 \in \mathbb{Z}$ such that

$$p+qi = (p_1+q_1i)(p_2+q_2i).$$

Since p and q are co-prime, all of p_1, q_1, p_2 and q_2 are non-zero. So

$$(p+qi)^2 = (p_1+q_1i)^2(p_2+q_2i)^2.$$

If $p_1+q_1i \neq p_2+q_2i$, then we can obtain $r+is$ with $|r+is|^2 = |p+iq|^2$ and with $r\neq 0$, $s\neq 0$ and $\{r,s\}\not\subset\{\pm p,\pm q\}$ by taking

$$r+is = (p_1+iq_1)\overline{(p_2+iq_2)}.$$

Now consider the example of $65 = 5\times 13$. The rows with 5 and 13 in the last column have $2+i$ and and $3+2i$ respectively in the first columns. We have

$$(2+i)(3+2i) = 4+7i,\quad (2+i)(3-2i) = 8-i.$$

Since $|4+7i| = |7+4i|$, and $|8-i| = |8+i|$, this confirms that

$$|7+4i|^2 = |8+i|^2.$$

Now consider $85 = 5\times 17$. The row with 17 in the last column has $4+i$ in the first entry. We have

$$(2+i)(4+i) = 7+6i,\quad (2+i)(4-i) = 9+2i$$

It is easily checked that

$$|7+6i|^2 = 85 = |9+2i|^2.$$

Of course $(9,2)$ is not in the table given, but does appear if the table is extended. We do not get a second triple from $25 = 5^2$, because 25 is not a product of distinct primes. But the row ending in 5 has $2+i$ in the first entry, and the row ending in 25 has $4+3i$ in the first entry. It is easily checked that

$$(2+i)^2 = 3+4i$$

and of course $|3+4i| = |4+3i|$.

5.

a) If one of a and b is odd and the other is even, then a^2-5b^2 is odd. So either both a and b are odd or both even. If they are both even then $a^2\equiv 0 \mod 4$ and $b^2\equiv 0 \mod 4$, and hence $a^2-5b^2\equiv 0 \mod 4$. If they are both odd then $a^2\equiv 1 \mod 8$ and $b^2\equiv 1 \mod 8$. Since also $5\equiv 1 \mod 4$, we have $a^2-5b^2\equiv 1-5\times 1\equiv 4 \mod 8$.

b) Suppose $2 = cd$ for c and $d\in\mathbb{Z}[\sqrt{5}]$ or c, $d\in\mathcal{O}[\sqrt{5}]$. Then $v(2) = 4 = v(c)v(d)$. By a) v cannot take the value ± 2. If $v(c) = 2$ and $c\in\mathcal{O}[\sqrt{5}]\setminus\mathbb{Z}[\sqrt{5}]$, then this follows from $c = (e_1+e_2\sqrt{5})/2$ where e_1 and e_2 are both odd integers, so that $e_1^2-5e_2^2$ cannot take the value ± 8. So without loss of generality $v(c) = 4$ and $v(d) = 1$, that is, d is a unit in $\mathbb{Z}[\sqrt{5}]$ (or $\mathcal{O}[\sqrt{5}]$. So 2 is irreducible in $\mathbb{Z}[\sqrt{5}]$ (or $\mathcal{O}[\sqrt{5}]$).

It is also possible to argue directly that if $2 = (c_1+c_2\sqrt{5})(d_1+d_2\sqrt{5})$ for integers c_1, c_2, d_1 and d_2, with both c_1 and $c_2\neq 0$, then $(d_1,d_2) = k(c_1,-c_2)$ for an integer k. I saw solutions which appeared to assume this, but without proof. It can be proved, but is not very quick and easy. To see it:

$$2 = (c_1d_1+5c_2d_2+\sqrt{5}(c_2d_1+c_1d_2),$$

and hence $c_2d_1+c_1d_2 = 0$. So $d_2/c_2 = -d_1/c_1$ and $(d_1,d_2) = (d_1/c_1)(c_1,-c_2)$ Since c_1 and c_2 have to be coprime, d_1/c_1 must be an integer. A similar result holds if c_1, c_2 d_1 and d_2 are half integers. In that case, d_1/c_1 can be a half integer.

c)

$$(\sqrt{5}-1)(1+\sqrt{5}) = 4 = 2^2.$$

2 and $\sqrt{5}-1$ and $\sqrt{5}+1$ are all inequivalent irreducibles in $\mathbb{Z}[\sqrt{5}]$, because the only units in $\mathbb{Z}[\sqrt{5}]$ are ± 1. But $(\sqrt{5}\pm 1)/2$ are units in $\mathcal{O}[\sqrt{5}]$, and so since

$$2 = (\sqrt{5}-1)((\sqrt{5}+1)/2) = (\sqrt{5}+1)((\sqrt{5}-1)/2,$$

all three of 2, $\sqrt{5}+1$ and $\sqrt{5}-1$ are equivalent irreducibles in $\mathcal{O}[\sqrt{5}]$ (in fact, equivalent primes, because $\mathcal{O}[\sqrt{5}]$ is a unique factorisation domain).