# MATH342 Feedback and Solutions 11

**1.**

a) By quadratic reciprocity, we have

$$\left(\frac{-7}{p}\right) = (-1)^{-4(p-1)/2}\left(\frac{p}{-7}\right) = \left(\frac{p}{-7}\right)$$

But $\left(\frac{p}{-7}\right)$ is 1 if and only if $p$ is a square mod $-7$, that is, a square mod 7, that is, $p = 1$, 2 or 4 mod 7.

*Quadratic reciprocity works for negative integers as well as positive ones. Of course, it is acceptable to write* $-7 = 7 \times (-1)$ *and consider* $\left(\frac{7}{p}\right)$ *and* $\left(\frac{-1}{p}\right)$ *separately, but it takes longer.*

b) If $p > 7$ is any integer (not necessarily prime) and $p = a^2 + 7b^2$ for integers $a$ and $b$ then $p \equiv a^2$ mod 7, and hence $p$ is congruent to 1, 2 or 4 mod 7. (this does not use part a).

c) From part a) we see that if $p$ is congruent to 1, 2 or 4 mod 7, then there is an integer $c$ such that $-7 \equiv c^2 \bmod p$, that is, $c^2 + 7 \equiv 0 \bmod p$, that is, $c^2 + 7$ is divisible by $p$.

**2.** The odd primes less than 100 which are congruent to 1, 2 or 4 mod 7 are:

$$11 = 2^2+7\times 1^2,\ \ 23 = 4^2+7\times 1^2,\ \ 29 = 1^2+7\times 2^2,\ \ 37 = 3^2+7\times 2^2,\ \ 43 = 6^2+7\times 1^2,\ \ 53 = 5^2+7\times 2^2,$$

$$67 = 2^2 + 7 \times 3^2,\ \ 71 = 8^2 + 7 \times 1^2,\ \ 79 = 4^2 + 7 \times 3^2.$$

**3.** If $a$ and $b$ are both odd integers, write $a^2 = 8m + 1$ and $b^2 = 8n + 1$. Then $a^2 + b^2 = 8(m + 7n) + 8$. So $(a/2)^2 + (b/2)^2 = 2(m + 7n) + 2$ is even, that is $|(a/2) + (b/2)\sqrt{-7}|^2$ is an even integer. Any element of $\mathcal{O}[\sqrt{-7}]$ is either of this form, or is of the form $c + d\sqrt{-7}$ for integers $c$ and $d$. It is obvious that $|c + d\sqrt{-7}|^2 = c^2 + 7d^2$ is an integer. So $|z|^2$ is an integer for all $z \in \mathcal{O}[\sqrt{-7}]$.

**4.** Suppose that $z = a + b\sqrt{-7} = a + b\sqrt{7}i$ divides the integer $m$ in $\mathcal{O}[\sqrt{-7}]$. Then$m = zw$ for some $w \in \mathcal{O}[\sqrt{-7}]$. Taking complex conjugation, $m = \overline{m} = \overline{zw}$. Since $\overline{z} = a - b\sqrt{-7} = a - b\sqrt{7}i$, it follows that $a - b\sqrt{-7}$ also divides $m$. If both $a$ and $b$ are nonzero, then $a - b\sqrt{-7} \neq \pm(a + b\sqrt{-7})$. If $a + b\sqrt{-7} = z$ is prime in $\mathcal{O}[\sqrt{-7}]$ then $\overline{z} = a - b\sqrt{-7}$ is too, because if $\overline{z} = w_1w_2$ then $z = \overline{w_1w_2}$, and if $\overline{w_j}$ is $\pm 1$, the same is true for $w_j$. So if $a + b\sqrt{-7}$ is prime in $\mathcal{O}[\sqrt{-7}]$ with both $a$ and $b$ non-zero, then $a - b\sqrt{-7}$ is an inequivalent prime. If one of them divides the integer $m$, then they both do, and hence, by unique factorisation, their product $a^2 + 7b^2$ also divides $m$.

**5.** Let $p$ be any odd prime which is congruent to 1, 2 or 4 mod 7. Then by 1c) there are integers $n$ and $c$ such that

$$np = c^2 + 7 = |c + \sqrt{-7}|^2.$$

Since $\mathcal{O}[\sqrt{-7}]$ is a unique factorisation domain, one of the primes $z = a + b\sqrt{-7}$ which divides $c + \sqrt{-7}$ must divide $p$. So then $|z|^2 = a^2 + 7b^2$ must divide $p$, by question 4. Since $p$ is prime, we must have $p = a^2 + 7b^2$. Since $p$ is odd, by question 3, $a$ and $b$ are integers, not just half integers.