MODEL ANSWERS TO THE FOURTH HOMEWORK

1. As d' divides a and b, by the universal property of d, $d'|d$. By symmetry d divides d'. But then d and d' are associates.
2. (a) As R is a UFD, we may factor a and b as

$$a = up_1^{m_1}p_2^{m_2}\cdots p_k^{m_k} \qquad \text{and} \qquad b = vp_1^{n_1}p_2^{n_2}\cdots p_k^{n_k},$$

where $p_1, p_2, \dots, p_k$ are primes, $m_1, m_2, \dots, m_k$ and $n_1, n_2, \dots, n_k$ are natural numbers, possibly zero, and u and v are units. Define

$$m = p_1^{o_1}p_2^{o_2}\cdots p_k^{o_k}$$

where o_i is the maximum of m_i and n_i. It follows easily that $a|m$ and $b|m$.
Now suppose that $a|m'$ and $b|m'$. Then, possibly enlarging our list of primes, we may assume that

$$m' = wp_1^{r_1}p_2^{r_2}\cdots p_k^{r_k},$$

where w is a unit and $r_1, r_2, \dots, r_k$ are positive integers. As $a|m'$, $r_i \geq m_i$. Similarly as $b|m'$, $r_i \geq n_i$. It follows that $r_i \geq o_i = \max(m_i, n_i)$. Thus m is indeed an lcm of a and b. Uniqueness of lcms' up to associates, follows as in the proof of uniqueness of gcd's.
(b) It suffices to prove this result for one choice of gcd d and one choice of lcm m. Pick d as in class (that is, take the minimum exponent) and take m as above (that is, the maximum exponent). In this case I claim that dm and ab are associates. It suffices to check this prime by prime, in which case this becomes the simple rule,

$$m + n = \max(m, n) + \min(m, n)$$

where m and n are integers.
3. (a) As $x+4$ has degree one, either it divides $x^3 - 6x + 7$ or these two polynomials are coprime. But if $x + 4$ divides $x^3 - 6x + 7$ then $x = -4$ is a root of $x^3 - 6x + 7$, which it obviously is not. Thus the gcd is 1.
(b) We have $x^7 - x^4 = x^4(x^3 - 1)$. Hence

$$\begin{aligned} x^7 - x^4 + x^3 - 1 &= x^4(x^3 - 1) + x^3 - 1 \\ &= (x^3 - 1)(x^4 + 1). \end{aligned}$$

Thus the gcd is $x^3 - 1$.

4. We apply Euclid's algorithm. $135-14i$ has smaller absolute value than $155+34i$. So we try to divide $155+34i$ by $135-14i$.

$$\begin{aligned}\frac{155+34i}{135-14i} &= \frac{(155+34i)(135+14i)}{135^2+14^2} \\ &= \frac{(135\cdot 155-34\cdot 14)+(155\cdot 14+135\cdot 34)i}{135^2+14^2}.\end{aligned}$$

The closest Gaussian integer is 1. The remainder is then

$$155+34i-(135-14i)1 = 20+48i.$$

So now we want to find the greatest common divisor of $135-14i$ and $20+48i$. We try to divide $20+48i$ into $135-14i$.

$$\begin{aligned}\frac{135-14i}{20+48i} &= \frac{(135-14i)(20-48i)}{20^2+48^2} \\ &= \frac{(135\cdot 20-48\cdot 14)-(135\cdot 48+14\cdot 20)i}{20^2+48^2}.\end{aligned}$$

The closest Gaussian integer is $1-2i$. The remainder is then

$$135-14i-(20+48i)(1-2i) = (135-20-96)+(-14-48+40)i = 19-22i.$$

So now we want to find the greatest common divisor of $19-22i$ and $20+48i$. So we try to divide $20+48i$ by $19-22i$.

$$\begin{aligned}\frac{20+48i}{19-22i} &= \frac{(20+48i)(19+22i)}{19^2+22^2} \\ &= \frac{(20\cdot 19-48\cdot 22)+(20\cdot 22+48\cdot 19)i}{19^2+22^2}.\end{aligned}$$

The closest Gaussian integer is $-1+2i$. The remainder is then

$$20+48i-(19-22i)(-1+2i) = (20+19-44)+(48-22-38)i = -5-12i.$$

So now we want to find the greatest common divisor of $19-22i$ and $-5-12i$. So we try to divide $-5-12i$ into $19-22i$.

$$\begin{aligned}\frac{20+48i}{-5-12i} &= -\frac{(19-22i)(5-12i)}{5^2+12^2} \\ &= \frac{(22\cdot 12-19\cdot 5)+(19\cdot 12+5\cdot 22)i}{5^2+12^2} \\ &= 1+2i.\end{aligned}$$

As there is no remainder, the greatest common divisor of $135-14i$ and $155+34i$ is $5+12i$.

5. It is convenient to introduce the norm, $N(\alpha)$, of any element of $\mathbb{Z}[\sqrt{-5}]$. In fact it is not harder to do the general case $\mathbb{Z}[\sqrt{d}]$, where d is any square-free integer. Given $\alpha = a+b\sqrt{d}$, the norm is by definition

$$N(\alpha) = a^2 - b^2 d.$$

Using the well-known identity,

$$A^2 - B^2 = (A+B)(A-B),$$

note that the norm can be rewritten,

$$N(\alpha) = (a+b\sqrt{d})(a-b\sqrt{d}) = \alpha\bar{\alpha},$$

where $\bar{\alpha}$, known as the conjugate of α, is by definition $a - b\sqrt{d}$. Note that in the case $d < 0$, in fact $\bar{\alpha}$ is precisely the complex conjugate of α. The key property of the norm, which may be checked easily, is that it is multiplicative (this is automatic when $d < 0$). Suppose that $\gamma = \alpha\beta$, then

$$N(\gamma) = N(\alpha)N(\beta).$$

Indeed if $\alpha = a + b\sqrt{d}$ and $\beta = a' + b'\sqrt{d}$, then

$$\gamma = (aa' + bb'd) + (a'b + ab')\sqrt{d},$$

so that

$$\begin{aligned} N(\gamma) &= (aa' + bb'd)^2 - d(a'b + ab')^2 \\ &= (aa')^2 + (bb')^2 d^2 - d(a'b)^2 - d(ab')^2. \end{aligned}$$

On the other hand

$$\begin{aligned} N(\alpha)N(\beta) &= (a^2 - b^2 d)((a')^2 - (b')^2 d) \\ &= (aa')^2 + (bb')^2 d^2 - d(a'b)^2 - d(ab)^2 \\ &= N(\gamma). \end{aligned}$$

We first use this to determine the units. Note that if α is a unit, then there is an element β such that $\alpha\beta = 1$. Thus

$$N(\alpha)N(\beta) = N(\alpha\beta) = N(1) = 1,$$

so that $N(\alpha)$ and $N(\beta)$ are divisors of 1. Thus if $\alpha = a + b\sqrt{d}$ is unit, then $a^2 - b^2 d = \pm 1$. Conversely, if the norm of α is ± 1, then $\mp\bar{\alpha}$ is the inverse of α. It follows that the units are precisely those elements whose norm is ± 1.

(a) As $d = -5$, the units are precisely those elements $\alpha = a + b\sqrt{-5}$ such that

$$a^2 + 5b^2 = 1.$$

The only possibilities are $a = \pm 1$, $b = 0$, so that $\alpha = \pm 1$. Suppose that 2 is not irreducible, so that $2 = \alpha\beta$, where α and β are not units. Then

$$4 = N(2) = N(\alpha)N(\beta).$$

As α and β are not units, then $N(\alpha)$ and $N(\beta)$ are greater than one. It follows that $N(\alpha) = N(\beta) = 2$. Suppose that

$$a^2 + 5b^2 = 2.$$

Then $b = 0$ and $a = \pm\sqrt{2}$, not an integer. Thus 2 is irreducible. For 3, the proof proceeds verbatim, with 2 replacing 3. The crucial observation is that one cannot solve

$$a^2 + b^2 = 3.$$

where a and b are integers. For $1 + \sqrt{5}$, observe that its norm is 6, so that α and β are of norm 2 and 3, which we have already seen is impossible.
(b) It suffices to prove that every ascending chain of principal ideals stabilises. But this is clear, since if

$$\langle \alpha \rangle \subset \langle \beta \rangle,$$

then

$$N(\beta) \leq N(\alpha),$$

with equality in one equation if and only if there is equality for the other. Thus a strictly increasing chain of principal ideals is the same thing as a strictly decreasing chain of natural numbers. Thus the set of principal ideals satisfies ACC as the set of natural numbers satisfies DCC.
(c) By (a),

$$6 = 2 \cdot 3 = (1 + \sqrt{-5})(1 - \sqrt{-5}),$$

are two different factorisations of 6 into irreducibles.

Challenge Problems: (Just for fun)

6. Say that S has the **cancellation property** if whenever $a+b = a+c$ then $b = c$. This is the natural analogue of the condition that there are no zero divisors in the ring; it is equivalent to saying that S can be embedded in a group.
Say that a and b are **associates** if $a = b + c$ and $a + d = b$ for some c and d.
Say that p is **prime** if whenever $p + c = a + b$ then either $p + d = a$ or $p + d = b$ for some d.

We say that S has **unique factorisation** if every non-zero element a of S, not a unit, is a sum of primes, unique up to re-ordering and associates.

7. First thin out the sequence $v_1, v_2, \dots, v_n$ by discarding any elements which are positive integral linear combinations of the other vectors. The remaining vectors are then all irreducible.

In this case I claim that S has unique factorisation if and only if $v_1, v_2, \dots, v_n$ are independent as vectors in the vector space $\mathbb{Q}^2$. In particular if S has unique factorisation then $n \leq 2$ and if there are two vectors, then neither is a multiple of the other.

Indeed suppose that we don't have unique factorisation. Then there is $v \in \mathbb{Z}^2$ such that,

$$v = \sum a_i v_i = \sum b_i v_i,$$

where $a_i \neq b_i$ for some i and $a_1, a_2, \dots, a_n$ and $b_1, b_2, \dots, b_n$ are positive integers. Subtracting one side from the other, exhibits a linear dependence between $v_1, v_2, \dots, v_n$. Conversely, suppose that $v_1, v_2, \dots, v_n$ are linearly dependent. Then we could find rational numbers $c_1, c_2, \dots, c_n$, not all zero, so that

$$\sum c_i v_i = 0.$$

Separating into positive and negative parts, $a_1, a_2, \dots, a_n$ and $b_1, b_2, \dots, b_n$ and putting the negative part on the other side, we would have

$$\sum a_i v_i = \sum b_i v_i,$$

for some positive rational numbers $a_1, a_2, \dots, a_n$ and $b_1, b_2, \dots, b_n$. Multiplying through by a highly divisible positive integer, we could clear denominators, so that $a_1, a_2, \dots, a_n$ and $b_1, b_2, \dots, b_n$ are integers. But then unique factorisation fails.

8. Let k be a field and let S be the infinite polynomial ring

$$k[x_1, x_2, \dots].$$

Let I be the ideal generated by $x_1x_2 = x_3x_4x_5$ and $x_4x_5 = x_6x_7x_8$, $x_7x_8 = x_9x_{10}x_{11}$ and so on. Let R be the ring S/I. It is not hard to show that $x_1, x_2, \dots$ are irreducible and that every element is a product of irreducibles.

Consider $a = x_1x_2 \in R$. Then x_1 and x_2 are irreducible and so a is a product of irreducibles. But $x_1x_2 = x_3x_4x_5$, so that a is also a product of x_3, x_4 and x_5. As $x_4x_5 = x_6x_7x_8$ we can keep going and the factorisation algorithm does not terminate starting with a.