MODEL ANSWERS TO THE FIFTH 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 $5+12i$.