MA2215: Fields, rings, and modules
Homework problems due on October 29, 2012

1. (**a**) Of course, if $\overline{a} \cdot \overline{b} = 1$ in $\mathbb{Z}/12\mathbb{Z}$, we have $ab = 1 + 12k$ in $\mathbb{Z}$, which immediately shows that a can only be invertible if a is coprime to 12, and all these elements are invertible. Therefore the answer is $\overline{1}$, $\overline{5}$, $\overline{7}$, $\overline{11}$.

(**b**) No. If $\overline{8} \cdot \overline{a} = \overline{9}$ in $\mathbb{Z}/12\mathbb{Z}$, we have $8a = 9 + 12k$ in $\mathbb{Z}$, so $9 = 8a - 12k$ is even, a contradiction. Therefore, $\overline{9}$ is not even a multiple of $\overline{8}$, let alone associate.

(**c**) Suppose that $b = ac$ and $a = bd$, where $c, d \in R$. We have $b = ac = bdc$, so we conclude that either $b = 0$ or $1 = dc$ since R is an integral domain, and we can cancel nonzero factors. If $b = 0$, then $a = bd = 0$, and $a = b$, so they are associates. Otherwise, $1 = dc$, so $c, d \in R^{\times}$, and so a and b are associates.

2. (**a**) The elements of our ring are $\overline{0}$, $\overline{1}$, $\overline{2}$, $\overline{3}$, $\overline{4}$, $\overline{5}$, $\overline{6}$, $\overline{7}$, $\overline{8}$, $\overline{9}$, $\overline{10}$, $\overline{11}$. Among those $\overline{1}$, $\overline{5}$, $\overline{7}$, $\overline{11}$ are invertible, so they are divisors of any element. Also, $\overline{2} \cdot \overline{3} = \overline{6}$, $\overline{9} \cdot \overline{10} = \overline{6}$, $\overline{6} \cdot \overline{1} = \overline{6}$, so the only elements that aren't obviously divisors are $\overline{0}$, $\overline{4}$, and $\overline{8}$. Any multiple of these elements is one of these elements again, since these are remainders of integers from $4\mathbb{Z}$, and a homomorphic image of an ideal is an ideal. Therefore, these elements are not divisors of $\overline{6}$, and the answer is $\overline{1}$, $\overline{2}$, $\overline{3}$, $\overline{5}$, $\overline{6}$, $\overline{7}$, $\overline{9}$, $\overline{10}$, $\overline{11}$.

(**b**) By definition of a greatest common divisor, d_1 is a divisor of d_2 and d_2 is a divisor of d_1, so by previous question (1c) they are associates.

3. Clearly, the set of all combinations of $ax + by$ is closed under sums and multiplication by any other element: $(ax_1 + by_1) + (ax_2 + by_2) = a(x_1 + x_2) + b(y_1 + y_2)$, $(ax + by)r = a(xr) + b(yr)$, so that set is an ideal. Since R is a PID, that ideal is generated by one element c. Since $a = a \cdot 1 + b \cdot 0$ and $b = a \cdot 0 + b \cdot 1$, c is a common divisor of a and b. Also, $c = ap + bq$ for some p and q, so if d is a common divisor of a and b, we can factor it out and conclude that $d \mid c$. Therefore, c is a greatest common divisor.

4. The set of all multiples is a square lattice generated by the vectors $(2, 1)$ and $(-1, 2)$. Clearly, $z_1 + (2 + i)\mathbb{Z}[i] = z_2 + (2 + i)\mathbb{Z}[i]$ if and only if $z_1 - z_2$ differ by a vector from that lattice, which means that for representatives of cosets we can take 0 and all points strictly inside one of the squares. By inspection, there are exactly 4 points inside one of each square, so the quotient ring consists of 5 elements.