Solutions to tutorial questions from October 18, 2012

1. *Answer*: t, $t+1$, t^2+t+1. Indeed, polynomials of degree 1 are always irreducible, since polynomials of degree 0 are invertible, and the product of two polynomials of degree 1 is of degree 2. Also, $t \cdot t = t^2$, $t(t+1) = t^2+t$, and $(t+1)^2 = t^2+2t+1 = t^2+1$, since we work in $\mathbb{Z}/2\mathbb{Z}$. These are all products of polynomials of degree 1, and what remains is the list of irreducibles. In this case, we see that t^2+t+1 is the only irreducible polynomial of degree 2.

2. Suppose that z is invertible, so that $zw = 1$. In class, we noted that for $d(a+bi) = a^2+b^2$, we have $d(zw) = d(z)d(w)$, so in our case $d(z)d(w) = d(1) = 1$. Since $d(z)$ assumes non-negative integer values, $d(z) = 1$, so $a = \pm 1$, $b = 0$ or $a = 0$, $b = \pm 1$, and the statement follows.

3. *Answer*: $7i$. Indeed, if $z = ab$, then $d(z) = d(a)d(b)$, so when looking for factorisations of a Gaussian integer it makes sense to factorise its norm. We have $d(2) = 4$, so we should look for Gaussian integers of norm 2. Such integers are $\pm 1 \pm i$, and indeed $(1+i)(1-i) = 2$, so 2 is not irreducible. Also, $d(3+i) = 10$, so possible divisors may have norms 5 and 2. In fact, if we take $1+i$ of norm 2 as a candidate divisor, we see that $\frac{3+i}{1+i} = 2-i$, so $3+i$ is not irreducible. Finally, $d(7i) = 49$, so a factorisation would have to have two factors of norm 7 each, but $7 = a^2+b^2$ with integers a and b is impossible. So $7i$ is irreducible.

4. Let us perform the Euclidean Algorithm. In $\mathbb{C}$, we have $\frac{b}{a} = \frac{70}{29} - \frac{1}{29}i$; rounding to closest integers, we get $2+0i$ as a candidate for q, and $r = b - aq = 5+5i$. Now we do the same with $a = 11+13i$ and $r = 5+5i$. We have $\frac{a}{r} = \frac{12}{5} + \frac{1}{5}i$; rounding to closest integers, we get $2+0i$ as a candidate for q_1 (same number again, purely coincidental!), and $r_1 = a - rq_1 = 1+3i$. Finally, $\frac{r}{r_1} = 2-i$, so r is divisible by r_1, and r_1 is a greatest common divisor.

For the optional question, the key idea is to notice that the set of multiples of an element $z \in E$ is a triangular lattice made of regular triangles with side $|z|$, and to use that for explaining the Euclidean domain property. We shall not discuss it in detail here.