MA2215: Fields, rings, and modules Homework problems due on October 22, 2012

1. It is enough to check that the maps $S \mapsto S/I$ and $\tilde{S} \mapsto \pi^{-1}(\tilde{S})$ that implement the one-to-one correspondence take ideals to ideals. To show that S/I is an ideal whenever S is, we need to show that (r + I)(s + I) and (s + I)(r + I) belong to S/I whenever s + I does. But (r + I)(s + I) = rs + I and (s + I)(r + I) = sr + I, so our statement follows from the fact that S is an ideal. The other way round, if \tilde{S} is an ideal of R/I, and $s \in \pi^{-1}(\tilde{S})$, then s + I is in \tilde{S} , so (r + I)(s + I) and (s + I)(r + I) belong to \tilde{S} whenever s + I does. But (r + I)(s + I) = rs + I and (s + I)(r + I) belong to \tilde{S} whenever s + I does. But (r + I)(s + I) = rs + I and (s + I)(r + I) belong to \tilde{S} whenever s + I does. But (r + I)(s + I) = rs + I and (s + I)(r + I) belong to \tilde{S} whenever s + I does. But (r + I)(s + I) = rs + I and (s + I)(r + I) = sr + I, so we conclude that rs and sr belong to $\pi^{-1}(\tilde{S})$.

2. Answer: t, t + 1, t - 1, t² + t - 1, t² - t - 1, and t² + 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, $t \cdot t = t^2$, $t(t + 1) = t^2 + t$, $t(t - 1) = t^2 - t$, $(t+1)(t-1) = t^2 - 1$, $(t+1)^2 = t^2 + 2t + 1 = t^2 - t + 1$, and $(t-1)^2 = t^2 - 2t + 1 = t^2 + t + 1$ since we work in $\mathbb{Z}/3\mathbb{Z}$. These are all products of polynomials of degree 1, and what remains is the list of irreducibles. In this case, we see that $t^2 + t - 1$, $t^2 - t - 1$, and $t^2 + 1$ are the three irreducible polynomials of degree 2.

3. Answer: 4 + i. 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(13) = 169, so we should look for Gaussian integers of norm 13. We instantly find (3-2i)(3+2i) = 13, so 13 is not irreducible. Also, d(3+4i) = 25, so possible divisors may have norm 5. In fact, if we take 2 + i of norm 5 as a candidate divisor, we see that $\frac{3+4i}{2+i} = 2 + i$, so 3 + 4i is not irreducible. Also, d(4+i) = 17, so it has to be irreducible. Finally, d(5+3i) = 34, and if we take 1 + i as a candidate divisor, we see that $\frac{5+3i}{1+i} = 4 - i$, so 5 + 3i is not irreducible.

4. Let us perform the Euclidean Algorithm. In \mathbb{C} , we have $\frac{13+33i}{19+9i} = \frac{16}{13} + \frac{15}{13}i$; rounding to closest integers, we get 1 + i as a candidate for q, and r = b - aq = 3 + 5i. Now we do the same with a = 19 + 9i and r = 3 + 5i. We have $\frac{a}{r} = 3 - 2i$, so a is divisible by r, and r is a greatest common divisor.

5. Performing long division, we see that

$$2t^4 - 7t^3 - 2t^2 + 5t + 7 = (2t^3 - 11t^2 + 8t + 21)(t + 2) + (12t^2 - 32t - 35),$$

and then

$$2t^3 - 11t^2 + 8t + 21 = (t/6 - 17/36) * (12t^2 - 32t - 35) - 23/18t + 161/36$$

Finally, $12t^2 - 32t - 35$ is divisible by -23/18t + 161/36 = -23/36(2t - 7), so we can pick 2t - 7 as a greatest common divisor.