Solutions to HW3

1. (a) $2+3\sqrt{2}$
   (b) $1+4\sqrt{2}$
   (c) $1+\sqrt{2}$
   (d) $\frac{4+\sqrt{2}}{3+2\sqrt{2}} \cdot \frac{3-2\sqrt{2}}{3-2\sqrt{2}} = \frac{3}{1} = 3$
   (e) 3

2. There are exactly $\phi(24) = 8$ choices of γ as primitive element:

   $$1+2\sqrt{2}, \quad 1+3\sqrt{2}, \quad 2+\sqrt{2}, \quad 2+4\sqrt{2}, \quad 3+\sqrt{2}, \quad 3+4\sqrt{2}, \quad 4+2\sqrt{2}, \quad 4+3\sqrt{2}.$$

   In order to check that γ is a generator in a cyclic group of order 24, it suffices to check that $\gamma^8 \neq 1$ and $\gamma^{12} \neq 1$.

3. (a) There are p^2 monic polynomials of degree two, $x^2+bx+c \in \mathbb{F}_p[x]$, corresponding to the choices of $b, c \in \mathbb{F}_p$. Of these, exactly $\binom{p}{2} = \frac{1}{2}p(p+1)$ are reducible polynomials $(x-r)(x-s)$ corresponding to the choices of roots $r, s \in \mathbb{F}_p$, not necessarily distinct. This leaves $p^2 - \frac{1}{2}p(p+1) = \frac{1}{2}(p^2-p)$ irreducible monic polynomials of degree two.

   (b) There are p^3 monic polynomials of degree three, $x^3 + bx^2 + cx + d \in \mathbb{F}_p[x]$, corresponding to the choices of $b, c, d \in \mathbb{F}_p$. This includes

   - $\frac{1}{6}p(p+1)(p+2)$ polynomials having three linear factors $(x-r)(x-s)(x-t)$ where $r, s, t \in \mathbb{F}_p$ are not necessarily distinct; and
   - $p \cdot \frac{1}{2}(p^2-p) = \frac{1}{2}p^2(p-1)$ polynomials of the form $(x-r)(x^2+bx+c)$ where the quadratic factor x^2+bx+c is irreducible.

   This leaves $p^3 - \frac{1}{6}p(p+1)(p+2) - \frac{1}{2}p^2(p-1) = \frac{1}{3}(p^3-p)$ irreducible monic polynomials of degree three.

   You should check how we counted irreducible polynomials of degree 2 and 3 in the case $p = 2$ in class (by counting reducible polynomials in each case, and subtracting from the total number of monic polynomials), as this gives the idea for the formula in general. Check for $p = 2$: 1 irreducible polynomial x^2+x+1 of degree two, and 2 irreducible polynomials x^3+x+1 and x^3+x^2+1 of degree three, in agreement with predictions using our formulas.