Number Theory Problem Set 6

Michael Magee, `michael.magee@yale.edu`

Questions from Ireland and Rosen

Questions VI.2, VI.3, VI.5 (we used this in class), VI.16, VI.18, VI.20

Question 1

Recall that $\mathcal{O}_D$ is the ring of integers in $\mathbf{Q}(\sqrt{D})$. Find both the fundamental unit of $\mathcal{O}_D$ and also its norm for $D = 2, 3, 5, 7$.

Question 2

Let M be a (finite-dimensional) matrix with entries in $\mathbf{Z}$. Prove that the eigenvalues of M are algebraic integers and the eigenvectors of M can be chosen to have coordinates whose entries are algebraic numbers (in fact, algebraic integers).

Question 3

For prime q let $\mathbf{F}_q$ denote the finite field with q elements, in other words $\mathbf{F}_q := \mathbf{Z}/q\mathbf{Z}$. Show that the set of odd q for which $x^2 - 3 \in \mathbf{F}_q[x]$ has two distinct roots is a union of arithmetic progressions. Does this statement generalize to the polynomial $x^2 - p$ where p is a fixed odd prime? How?