Math 115 Fall, 2011

Professor K. A. Ribet

Assignment due November 10, 2011

Let p be an odd prime and write $\mathbf{F} = \mathbf{Z}/p\mathbf{Z}$ for the ring of integers mod p. Fix a non-zero element D of $\mathbf{F}$, and let $R = \mathbf{F}[\sqrt{D}]$. We think of R as the set of sums $a + b\sqrt{D}$ with a and b in F. Formally, it is the set of pairs $(a, b) \in \mathbf{F}^2$; in particular, R has p^2 elements. Addition is defined componentwise; multiplication is defined in the obvious way that takes account of the rule $\sqrt{D}\cdot\sqrt{D} = D$. Unless I've made a typing or other error, the formula is $(a, b)\cdot(c, d) = (ac+bdD, ad+bc)$. For $\alpha = a + b\sqrt{D} \in R$, we define $\overline{\alpha} = a - b\sqrt{D}$, as usual. If $D = -1$, we are mimicing the construction of $\mathbf{C}$ (starting with $\mathbf{R}$), including the usual complex conjugation.

A number $\alpha \in R$ is said to be *invertible* if there is a $\beta \in R$ for which $\alpha\beta = 1$.

a. Show that α is invertible if and only if $\alpha\overline{\alpha}$ is non-zero.

b. If D is a non-square in $\mathbf{F}$, show that α is invertible if and only if α is non-zero.

c. If D is a (non-zero) square, calculate the number of invertible elements of R.

Problems from the Book:

§4.2, problem 21

§7.1, problems 1, 3: do all parts by hand and then using `sage`.

§7.1, problem 5

§7.3, problems 1, 2, 3a