Math 115 | Professor Kenneth A. Ribet

Homework assignment #14
Due December 8, 2006

1. Let $\alpha = a + c\omega$ be an element of $\mathbf{Z}[\omega]$, and suppose that $\alpha\omega = b + d\omega$. (The quantities a, b, c and d are intended to be ordinary integers.) Show that $N(\alpha) = \det \begin{pmatrix} a & b \\ c & d \end{pmatrix}$.

2. Suppose that $\alpha \in \mathbf{Z}[\omega]$ is prime to 3 (i.e., to $\lambda = 1 - \omega$). Show that there is a unique unit $u \in \mathbf{Z}[\omega]$ such that $u \equiv \alpha \bmod 3$. (The congruence means that $u - \alpha$ is a multiple of 3 in $\mathbf{Z}[\omega]$.)

3. Suppose that p is a prime $\equiv 1 \bmod 3$. We proved in class on December 1 that there are integers n and m so that $4p = n^2 + 3m^2$. Was the coefficient 4 really necessary? Observe that $7 = 2^2 + 3 \cdot 1^2$, $13 = 1^2 + 3 \cdot 2^2$, $19 = 4^2 + 3 \cdot 1^2$, $31 = 2^2 + 3 \cdot 3^2, \ldots$, so it looks as if the coefficient "4" is not necessary. Prove that we can dispense with it, or else show that we do need to carry it along with us.

4. In the formula $4p = n^2 + 3m^2$ of the previous problem, show that we can choose m to be divisible by 3 and that n and m are unique up to sign if we make that choice. If we insist on the congruence $n \equiv 1 \bmod 3$ as well as the congruence $m \equiv 0 \bmod 3$, show that n is unambiguously defined as a function of p. Calculate the function $p \mapsto n$ for as many values of $p \equiv 1 \bmod 3$ as you can without getting bored or tired. (If you write a program and compute a big table, you won't get bored, but you might get tired.)

5. For as many prime numbers p as you can, calculate the number of solutions of the congruence $x^3 + y^3 \equiv 1 \bmod p$. The solutions are pairs of integers mod p that satisfy the congruence, so there are at most p^2 solutions. You might get a table that includes data like this:

p	7	13	19	31	$\cdots$
# solns.	6	6	24	33	$\cdots$.

Find a rule for the number of solutions when $p \equiv 2 \bmod 3$ and prove that your rule is correct. For $p \equiv 1 \bmod 3$, guess a rule that links the number of solutions mod p to the function $p \mapsto n$ of problem 4. Verifying that the rule is correct is much harder for $p \equiv 1 \bmod 3$ than for $p \equiv 2 \bmod 3$; Gauss did the verification in his mathematical diary.

Happy End of Semester to All!