Number Theory Fall 2009
Homework 9
Due: Wed. Nov. 4, start of class

Exercise 7.1. *Show* $\zeta_3^2 + \zeta_3 + 1 = 0$. *Using this, deduce that* $\mathbb{Z}[\zeta_3]$ *is closed under multiplication. (Note the set of integer linear combinations of 1 and* α, $\{a + b \cdot \alpha | a, b \in \mathbb{Z}\}$, *is not always closed under multiplication. For example when* $\alpha = \sqrt[3]{2}$ *or* $\alpha = e^{2\pi i/5}$, α^2 *is not a linear combination of 1 and* α.*)*

Exercise 7.2. *For* $\alpha \in \mathbb{Z}[\zeta_3]$, *let* $\overline{\alpha}$ *be the complex conjugate of* α, *and define the norm by* $N(\alpha) = |\alpha|^2 = \alpha\overline{\alpha}$. *(The norm of* $a + b\zeta_3$ *is* not $(a + b\zeta_3)(a - b\zeta_3)$.*) Show* $\overline{\alpha} \in \mathbb{Z}[\zeta_3]$ *for any* $\alpha \in \mathbb{Z}[\zeta_3]$. *Compute* $\overline{\zeta}_3, N(\zeta_3)$ *and* $N(1 + \zeta_3)$. *Write down a formula for* $N(a + b\zeta_3)$ *where* $a, b \in \mathbb{Z}$.

Exercise 7.3. *Determine the units of* $\mathbb{Z}[\zeta_3]$ *(the elements of norm 1).*

Exercise 7.4. *Exercise 7.4.1. This resolves the non-unique factorization of* $4 = 2 \cdot 2 = (1+\sqrt{-3})(1-\sqrt{-3})$ *in* $\mathbb{Z}[\sqrt{-3}]$ *by going to* $\mathbb{Z}[\zeta_3]$.

Exercise 7.5. *What are the possible remainders mod* $\pi = \sqrt{-3}$ *in* $\mathbb{Z}[\zeta_3]$*? (Hint: they will be the elements whose norm is less than that of* π.*) Show that for any* $z, x \in \mathbb{Z}$ *(or even* $\mathbb{Z}[\zeta_3]$*)* $z - x \equiv z - x\zeta_3 \equiv z - x\zeta_3^2$, *which we need in the proof of Fermat's Last Theorem for* $n = 3$. *(If you need at hint, look at p. 131.)*

Exercise 7.6. *Fermat's Last Theorem says* $x^n + y^n = z^n$ *has no solutions in* $\mathbb{N}$ *if* $n > 2$. *Show that if* $d|n$ *then a solution to* $x^n + y^n = z^n$ *give a solution to* $x^d + y^d = z^d$. *Deduce that Fermat's Last Theorem is true for* $n \equiv 0 \bmod 3$. *Also deduce that to prove Fermat's Last Theorem, it suffices to prove it for* $n = 4$ *and* $n = p$ *where* p *is any odd prime.*

Exercise 8.1. *Let* p *be an odd prime. We say* a *is a* square *or* quadratic residue *mod* p *if* $a \equiv x^2 \bmod p$ *for some* x. *Prove there are* $\frac{p+1}{2}$ *distinct squares mod* p.

Exercise 8.2. *Let* p *be an odd prime. Show* $x^2 + y^2 \equiv -1 \bmod p$ *for some* $x, y \in \mathbb{Z}$. *(Hint: use the previous exercise and the pigeonhole principle.)*