M445/845, Homework 2, due Friday, September 27, 2013

Instructions: Do any three problems.

(1) Euclid's proof that the integers have infinitely many primes goes like this. Consider any finite nonempty list $P = \{p_1, \ldots, p_r\}$ of primes p_i. Then $N = 1 + p_1 \cdots p_r$ is an integer bigger than 1, so N has a prime factor p. Since none of the primes p_i evenly divide N, we see p is not any of the p_i so p is a prime not on the list P. Thus the list P is not complete; i.e., no finite list of primes contains all of the primes, so there are infinitely many primes. Modify this proof to show that there are infinitely primes p leaving a remainder of 3 when divided by 4 (such as 3, 7, 11, 19, etc.).

(2) Look up Dirichlet's theorem on arithmetic progressions. Use its statement to prove both that there are infinitely many primes congruent to 3 modulo 4, and that there are infinitely many primes congruent to 1 modulo 4. Also explain why Dirichlet's theorem on arithmetic progressions doesn't also imply that there are infinitely many primes congruent to 2 modulo 4. (Primes congrunt to 2 modulo 4 would be even, so we know there can't be infinitely many such primes, but why does Dirchlet's theorem work for 1 or 3 mod 4 but not 2 mod 4?)

(3) Use the definition of what it means for an element of a domain to be prime to show if $m + ni \in \mathbf{Z}[i]$ is prime in the Gaussian integers $\mathbf{Z}[i]$, then $m - ni$ is also prime.

(4) (a) Factor $102 + 107i$ as a product of Gaussian primes.
(b) Find a quotient q and remainder r such that $a = bq + r$ with either $r = 0$ or $N(r) < N(b)$ when $a = 102 + 107i$ and $b = -40 + 73i$.
(c) Find a greatest common divisor for $a = 102 + 107i$ and $b = -40 + 73i$.

(5) Show that the ring of integers for the field $\mathbf{Q}$ of rationals is just the usual integers $\mathbf{Z}$ (i.e., show that a rational root of a monic polynomial in $\mathbf{Z}[x]$ must be an integer). [Hint: think about the rational root test.]

(6) It is an open problem to determine whether or not $n^2 + 1$ is prime for infinitely many integers n. Here are two easier problems of this sort.
(a) Show that there is only one prime of the form $n^4 + n^2 + 1$ for n an integer.
(b) Show that there is only one prime of the form $n^4 + 4$ for n an integer.

(7) For each real $r > 0$, let n_r be the number of Gaussian primes $m + ni$ such that $N(m + ni) = r^2$ (i.e., such that $m + ni$ is contained in the perimeter of the circle C_r of radius r with center at 0 in the complex plane $\mathbf{C}$). Show that n_r is either 0, 4 or 8, and that each value occurs for infinitely many r. (When doing the case of $n_r = 8$, you will along the way show that there are infinitely many Gaussian primes of the form $m + ni$ with $m \neq 0 \neq n$, and thus that there are infinitely many primes in $\mathbf{Z}$ congruent to 1 modulo 4.)