Math 328K (Rusin) – last homework set – due at day of final!

By popular demand I am making this homework set into a preparation for the final, too. So the questions are at least nominally concerned with the topics we are discussing at the end of the semester but also force you to think again about things we were discussing in September!

The set of *Gaussian integers* is the set $\mathbf{Z}[i]$ of complex numbers of the form $z = z_1 + i\,z_2$ where z_1 and z_2 are integers. It is clear that the sum, difference, or product of two of these is again of this form.

The Gaussian integers are *not* ordered, the way the ordinary integers are, but we still have a notion of size: we define $||z|| = \sqrt{z_1^2 + z_2^2}$. This has many of the same properties that the ordinary absolute value has, e.g. $||z \cdot w|| = ||z||\,||w||$ and $||z + w|| \le ||z|| + ||w||$. Note that when $z \in \mathbf{Z}[i]$, $||z|| \in \mathbf{Z}$. Thus two Gaussian integers can only multiply to 1 when each of them lies in the set $\{1, -1, i, -i\}$. These four Gaussian integers are called the *units* of $\mathbf{Z}[i]$.

1. Show that if $z, w \in \mathbf{Z}[i]$ and $w \neq 0$ then there are rational numbers x_1, x_2 such that $z = w \cdot (x_1 + i\,x_2)$. We call $x = x_1 + i\,x_2$ the "quotient" of z by w. (Hint: you can simplify fractions involving complex numbers using the identity $\dfrac{1}{u+vi} = \dfrac{u-vi}{u^2+v^2}$.)

2. Prove the following analogue for the Gaussian integers of the "Division Algorithm" we proved for the ordinary integers:

Theorem: For any two Gaussian integers $z, w \in \mathbf{Z}[i]$ with $w \neq 0$ there exist a pair of Gaussian integers $q, r \in \mathbf{Z}[i]$ satisfying

(i) $z = w \cdot q + r$

(ii) $||r|| < ||w||$

(Hint: you can find such a q by rounding the rational numbers x_i in problem 1, and then define r by (i). Note that if e_1 and e_2 are rational numbers with $|e_i| \le 1/2$, then $||e_1 + ie_2|| \le \sqrt{2}/2 < 1$.)

Interestingly, unlike the case for the ordinary integers, these q, r are *not* uniquely specified from the two conditions (i) and (ii). For example, we have both $(1 + 2i) = (3 + i)(0) + (1 + 2i)$ and $(1 + 2i) = (3 + i)(i) + (2 - i)$ — both remainders have magnitude $\sqrt{5}$ which is less than $||w|| = \sqrt{10}$. But q and r and *almost* unique — once one q is found, any others differ from it by ± 1 or $\pm i$ (which I encourage you to try to prove!)

When $z, w \in \mathbf{Z}[i]$, we say $w|z$ if there is another Gaussian integer v with $z = w \cdot v$. You should convince yourself that the familiar properties of this divisibility relationship hold (e.g. it is transitive).

3. Prove that every pair z, w of Gaussian integers has a gcd – another Gaussian integer which is divisible by every common divisor of z and w. (Hint: You can *define* the gcd to be the last nonzero term in the Euclidean Algorithm, that is, the last nonzero remainder in the repeated application of the Division algorithm. Then simply observe that if $v|z$ and $v|w$ then $v|(z - qw)$. So all the common divisors of z and w divide their gcd.)

Due to the nonuniqueness in the Division Algorithm, the gcd is also not unique! But any two gcd's must divide each other, which — you should prove this! — means each of the gcds is a unit times the other gcd.

It would not be a terrible thing to review how, for the ordinary integers, we went from the Division Algorithm, to the Euclidean Algorithm, to the existence of gcd's, to the Fundamental Theorem of Arithmetic. Having completed problems 1–3, you can then conclude in the same way that every Gaussian integer may be written as a product of Gaussian primes, in a way which is unique, up to order *and* up to multiplication by units. Here a Gaussian integer may equally well be defined by the Euclidean condition ("p is prime if $p|zw$ implies $p|z$ or $p|w$") or the irreducibilty condition ("p is prime if $p = zw$ implies z or w is a unit").

4. Show that the Gaussian integers $2 = 2 + 0i$ and $5 = 5 + 0i$ are not prime, and find a nontrivial factorization of each.

5. Suppose that p is an ordinary integer prime other than 2, but the Gaussian integer $p + 0i$ is not a Gaussian prime. Show that $p \equiv 1 \pmod 4$. (Hint: if $p + 0i = P_1 P_2 \dots P_n$ then $||p + 0i|| = ||P_1|| \, ||P_2|| \dots ||P_n||$, which means that $n = 2$ and each $||P_i|| = p$. This means that p can be written as a sum of two squares, and that means that $p \equiv 1 \bmod 4$.)

I have given you a one-sentence proof that, conversely, if $p \equiv 1 \bmod 4$ then there are integers x, y with $x^2 + y^2 = p$, so that $p = (x + iy)(x - iy)$ and therefore $p + 0i$ is not a Gaussian prime. That proof is not especially constructive, however. The remaining discussion will give you a way to find x and y.

Recall that if $p \equiv 1 \bmod 4$, then we have shown the Legendre symbol $(\frac{-1}{p}) = +1$, that is, there exist integers a with $a^2 \equiv -1 \bmod p$. These are not hard to find: if you pick a congruence class $[b]_p$ at random, and compute $a = b^{((p-1)/4)}$, then $a^4 \equiv 1 \bmod p$ so $a^2 \equiv \pm 1 \bmod p$; it turns out that the two possibilities occur equally often, and so after a few random choices of b you are highly likely to have found an a with $a^2 \equiv -1 \bmod p$, that is, you have found an integer a such that $p|(a^2 + 1) = (a + i)(a - i)$.

If P is a Gaussian prime which divides p, it then follows that P divides either $a + i$ or $a - i$ (and indeed it can be shown that p is the product of two primes, one dividing $a + i$ and the other dividing $a - i$). Thus P divides the Gaussian $\gcd(p, a + i)$. As noted above, p will actually be a product of just two Gaussian primes, and they don't *both* divide $a + i$, so this gcd is just a single Gaussian prime. Therefore, if we write $x + iy$ for this gcd, then $(x + iy)|p$, so that $x^2 + y^2 = p$. We have now written p as the sum of two squares!

6. Carry out this computation when $p = 29$. That is, find an integer a with $a^2 \equiv -1 \bmod 29$ and compute $\gcd(29, a + i)$ to find an integer solution to the quadratic Diophantine equation $x^2 + y^2 = 29$.

(Hint: yes, I am perfectly well aware that you don't need any great theory to find such an x and y ! But if you are a computer programmer you might want to carry out the steps above to find the x and y that correspond to $p = 12345678901234567894 9$ or some such prime.)