Math 113 Homework 1, due 2/5/2019

1. Write an addition table for the integers modulo 3 (it should have nine entries).

2. (a) Multiply the following complex numbers by i and by $-i$:

$$2 + i, -i, -\pi + e \cdot i, -\sqrt{2} - 2i.$$

(b) If $z = a + bi$ is a complex number, its *complex conjugate* is the number

$$\bar{z} := a - bi$$

with the imaginary part negated. Show that $z \cdot \bar{z} = a^2 + b^2$. (This implies in particular that it is a real, positive number.) Show (this should be easy) that $iz \cdot \bar{iz}$ gives the same answer as $z \cdot \bar{z}$.

(c) Find 8 distinct Gaussian numbers z such that $z \cdot \bar{z} = 5$ (remember that $z \in \mathbb{C}$ is a Gaussian number if $z = a + bi$ for $a, b \in \mathbb{Z}$). Note: the shorthand notation $\pm$ will be useful here; for example, $\pm 1 \pm i$ represents shorthand for a set of four different complex numbers!

(d) Find 12 distinct Gaussian numbers z such that $z \cdot \bar{z} = 25$. Hint: multiply together pairs of numbers in part (c).

(e) Show that there are no Gaussian numbers z such that $z \cdot \bar{z} = 3$ (hint: squares of nonzero integers are always ≥ 1).

3. (a) Check that multiplication of Gaussian numbers modulo $2 + i$ is well-defined, i.e. if $\alpha \sim \alpha'$ are Gaussian numbers which are equivalent modulo $2 + i$ (i.e. their difference is a Gaussian number divisible by $2 + i$) and $\beta \sim \beta'$ are two other Gaussian numbers which are equivalent to each other then $\alpha \cdot \alpha' \sim \beta \cdot \beta'$ and $\alpha + \alpha' \sim \beta + \beta'$. Hint: write $\alpha' = \alpha + \delta \cdot (2 + i)$, etc.

Remark: of course the specificity of working modulo $2 + i$ is not important here: we're using the example of $2 + i$ to check that modular arithmetic works for the Gaussian numbers.

(b) Remember that each Gaussian number is equivalent (modulo $2 + i$) to one of the five elements $\{0, 1, i, -1, -i\}$. Write down an addition table for the five classes of elements, namely $[0]$ (any element equivalent to 0), $[i]$ (any element equivalent to i) etc. So for example, $[0] + [i] = [i]$ (here the calculation works on the nose), but $[1] + [i] = [-1]$, since $1 + i$ is not on the liest but $1 + i \sim -1$ (their difference is $2 + i$), and -1 is. This table should have 25 entries (though half of them are immediate because of commutativity).

(c) Similarly, write down a multiplication table. (This will be surprisingly easy: this is a special nice property of residues modulo $2 + i$.)

4. (a) Now write down the addition table $\mathbb{Z}/5$, the integers modulo 5. Can you find an isomorphism

$$f : (\mathbb{Z}/5, +) \to (\mathbb{G}/(2 + i), +)$$

of binary structures from the integers modulo 5 with addition to the Gaussian integers modulo $2+i$ (from the previous problem), also with addition? Can you find another, different isomorphism? (To specify an isomorphism, write down a class of Gaussian integers modulo $2+i$ where each element of $\mathbb{Z}/5$ goes, and check a couple of nontrivial cases of the homomorphism property to convince yourself that this is actually an isomorphism.) Hint: if you first pick where $[1] \in \mathbb{Z}/5$ goes, you also know where $[2] = [1] + [1]$ goes by the homomorphism property, and then you know where $[3] = [2] + [1]$ goes, etc.

5. View 2 as a Gaussian number. Then if $\alpha = a + bi$ is another Gaussian number, then $2\alpha = 2a + 2bi$, so a Gaussian number is divisible by 2 if both of its components are even, and two Gaussian numbers are equal modulo 2 if their difference has even components. This gives four equivalence classes of Gaussian numbers modulo 2, namely:

$$\text{even } + \text{ even } \cdot i, \text{ odd } + \text{ even } \cdot i, \text{ even } + \text{ odd } \cdot 1, \text{ and odd } + \text{ odd } \cdot i.$$

We pick a "representative" Gaussian number in each class and write these in shorthand (in the same order) as $\{[0], [1], [i], [1+i]\}$. Now write addition and multiplication tables for the Gaussian numbers modulo 2.

6. Challenge problem: you can do this one instead of any two of the others, or you can do it as extra credit for an extra 10% on this HW.

(a) Show that any complex number is a distance of at most $\frac{\sqrt{2}}{2}$ away from a Gaussian number (hint: $\frac{\sqrt{2}}{2}$ is the distance from a vertex of the unit square to its center).

(b) Show that if α is a nonzero complex number, then any complex number z is at most $\frac{\sqrt{2}|\alpha|}{2}$ away from a multiple of α (hint: if z is distance d from $\lambda \cdot \alpha$ then $\frac{z}{\alpha}$ is distance $\frac{d}{|\alpha|}$ away from λ).

(c) Deduce that if $\alpha = a + bi$ is a nonzero Gaussian number then any other Gaussian number $z \in \mathbb{G}$ is equivalent modulo α to a Gaussian number of magnitude $< |\alpha|$ (remember that $|\alpha| = \sqrt{a^2 + b^2}$). This is a version of "division with remainder" for Gaussian numbers.

(d) This means that all "colors", or types of residue modulo α are contained in the interior of the circle of radius $|\alpha|$ (in fact, we've seen they are contained in the closed circle of radius $\frac{\sqrt{2}}{2}\alpha$). Give an example, however, where two such residues are the same (i.e. we are "overcounting").

Remark: from part (c) above, you can deduce that there are less than πr^2 residue classes modulo α, where $r^2 = |\alpha|^2 = a^2 + b^2$. This is nice, because it implies that there are finitely many possibilities for the residue, which was not obvious a priori. Part (d) shows that this estimate will tend to overcount. In fact this estimate is off by a constant. There is a beautiful formula for the total number of residues: it is exactly $a^2 + b^2$. While you don't have to do this, I would encourage you to check this formula when $\alpha = a + 0i$ is real and positive.