Math 185 Homework 1. Due Friday 1/31 (later homeworks due Wednesday)

1. Define $\exp(iy) := \cos(y) + i\sin(y)$.
a. Prove, using trigonometry, that $\exp(iy+iy') = \exp(iy)\cdot\exp(iy')$ for $y, y' \in \mathbb{R}$ two real numbers.

$\cos(y+y')+i\sin(y+y') = \cos^2(y)-\cos^2(y')+2i\sin(y)\sin(y') = (\cos(y)+i\sin(y))\cdot(\cos(y')+i\sin(y'))$.

b. Prove directly (using Taylor series for sin and cos) that

$$\exp(iy) = \sum_{n=0}^{\infty} \frac{(iy)^n}{n!},$$

where $n!$ denotes the factorial of n. Hint: you may use the fact that an infinite sum of complex numbers $\sum a_n$ converges if and only if $\sum \mathrm{Re}(a_n)$ and $\sum \mathrm{Im}(a_n)$ both converge and if it converges, $\sum a_n = \sum \mathrm{Re}(a_n) + i\sum \mathrm{Im}(a_n)$. Now apply this to $a_n = \frac{(iy)^n}{n!}$.

Even terms are real and only contribute to teh real part, odd terms are imaginary and only contribute to the imaginary part, so the sum is equal to $\sum_k \frac{(iy)^{2k}}{(2k)!} + i\sum_k \frac{(iy)^{2k+1}}{(2n+1)!}$. The real part is $\sum \frac{(-1)^k}{(2k)!}y^{2k}$ and the imaginary part is $i\cdot\sum_k \frac{(-1)^k}{(2n+1)!}y^k$

2. This and the following exercise are meant to help develop your thinking about complex numbers. They do not follow the book: you will need to think a bit on your own in order to solve these. For a positive real number $r \in \mathbb{R}$, define

$$C_r := \{z \mid \quad |z| = r\}$$

to be the circle of radius r around 0.

Let $\mathbb{G} = \{x + iy \mid x, y \in \mathbb{Z}\}$ (called the set of "Gaussian numbers") be the set of complex numbers with integer real and imaginary part.
a. Prove that the product $z \cdot z'$ of two elements $z, z' \in \mathbb{G}$ is again in $\mathbb{G}$.

$(a+bi)(a'+b'i) = aa' - bb' + (ab' + a'b)i$. If all coefficients are integers, then both $aa' - bb'$ and $ab' + a'b$ are integers as well.

b. Prove that $\mathbb{G} \cap C_1 = \{\pm 1, \pm i\}$. In other words, the only elements $z \in \mathbb{G}$ with $|z| = 1$ are the four distinct powers or i.

If $|a+bi| = 1$ then $a^2+b^2 = 1$. If a, b are integers, then a^2, b^2 are non-negative integers, and the only way two non-negative integers add to 1 is if one is equal to 1 and the other is zero. This means one of a, b is 0 and the other is ± 1, giving the four options $\pm 1, \pm i$.

From now on, we write $U_4 := \{\pm 1, \pm i\}$ (here U_4 stands for "fourth roots of unity").

c. Prove that if $|z| = r$ then $|uz| = r$ for $u \in U_4$ and $|\bar{z}| = r$. Let $C_r \subset \mathbb{C}$ be the circle of radius r, given by $C_r = \{z \in \mathbb{C} \mid |z| = r\}$. Show that $|C_r \cap \mathbb{G}|$ (the set of Gaussian integers of absolute value r) is finite and has number of elements divisible by 4[1]. (Hint: the set $\{\pm 1, \pm i\}$ has four elements).

Note that $z = a + bi$ is in $C_r \cap \mathbb{G}$ if and only if $|z| = r$ and $a, b \in \mathbb{Z}$. There are a finite number of such elements, since if $z \in C_r$ then $|a|, |b| \leq r$, and there are finitely many options for integers in this range. Clearly $\bar{z} = a - bi$ satisfies these properties. If $u \in U_4$, then $|u| = 1$ so $zu = |z||u| = |z| \cdot 1 = r$, and $zu \in \gg$ (is Gaussian) since Gaussian numbers are closed under product, so $zu \in C_r \cap \mathbb{G}$ as well.

Say an element z is in the first quadrant if its argument is in $[0, \pi/2)$ (equivalently, if $x \geq 0$ and $y > 0$), in the second quadrant if in $[\pi/2, \pi)$, and similarly for the third and fourth quadrants. Then observe that there is a unique element u_0 of U in the same quadrant as z (1 is in the first quadrant, i is in the second quadrant, -1 is in the third quadrant and -1 is in the fourth quadrant), and so $z \in C_r \cap \gg$ is in the n^{th} quadrant if and only if $z \cdot u_0^{-1}$ is in the first quadrant. So each quadrant of $C_r \cap \gg$ has the same number of elements, and the order of $C_r \cap \gg$ is divisible by 4.

d. Show that if (for two numbers $r, s \in \mathbb{R}$), the circles C_r and C_s both contain a Gaussian number then the circle C_{rs} also contains a Gaussian number. Deduce that if m, n are integers which can be expressed as the sum of two squares then mn can be as well (hint: show that m is the sum of two squares if and only if $C_{\sqrt{m}}$ contains a Gaussian number).

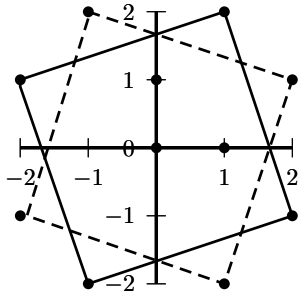
Assume there is $z \in C_r \cap \gg$, and $z' \in C_s \cap \gg$. Then since Gaussian numebrs are closed under product and absolute values multiply when taking product, we have the Gaussian number $zz' \in C_{rs} \cap \gg$. Note that there is a Gaussian numbers $z = a + bi$ in $C_{\sqrt{n}}$ if and only if $\sqrt{n} = \sqrt{a^2 + b^2}$ for a pair of integers a, b, i.e. if and only if n is a sum of squares. We've just shown that if n, m are sums of squares (i.e. $C_{\sqrt{m}}, C_{\sqrt{n}}$ both contain a Gaussian number) then so is nm.

e. Find all Gaussian numbers of length $\sqrt{5}$, i.e. all numbers in $C_{\sqrt{5}} \cap \mathbb{G}$. Sketch them (or draw them on graph paper.) Connect pairs of numbers which are related by multiplication by $\pm i$. (This should

[1] if $C_r \cap \mathbb{G}$ is empty, it has 0 elemnts, which is divisible by 4.

split your numbers into "squares").

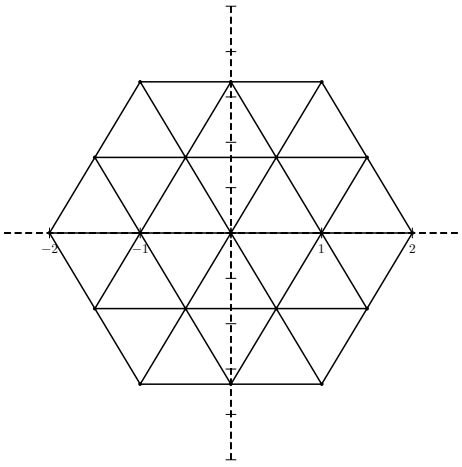
See diagram:



3. Now we do the same thing for the ring of *Eisenstein integers.* Define the set of Eisenstein integers $\mathbb{E}$ to be the set of integers $\mathbb{E} := \{\frac{a+b\sqrt{3}i}{2} \mid a \equiv b \mod 2$. So for example, $-5\sqrt{3}i \in \mathbb{E}$ and $3 - \sqrt{3}i \in \mathbb{E}$ bue $1 + \frac{\sqrt{3}}{2}$ is not in $\mathbb{E}$.

a. Draw a (sketch) of the Eisenstein integer lattice. (You should get something with hezagonal symmetry!) Show that the set of Eisenstein integers is closed under multiplication, so if $z, z' \in \mathbb{E}$, then so is $z \cdot z'$.

The lattice looks like the nodes in this figure:



Note that the condition $z = x+y\sqrt{3}i$ for $x, y \in \mathbb{Q}$ is equivalent to $z = a+b\zeta_6$, for $\zeta_6 = \frac{1+\sqrt{3}i}{2}$. The condition that $x, y \in \frac{\mathbb{Z}}{2}$ (integers or half-integgers) with $x \equiv y \mod 1$ is equivalent to the condition $a, b \in \mathbb{Z}$ above (why?). Thus the Eisenstein integers are the set of complex numbers of the form $a+b\zeta$. If $z = a+b\zeta$ and $z' = a'+b'\zeta$ then, using $\zeta^2 = \zeta - 1$ we have $zz' = aa' + (ab' + a'b)\zeta + bb'\zeta^2 = aa' - bb' + (ab' + a'b + bb')\zeta$.

Alternative proof: if $z = \frac{x+y\sqrt{3}i}{2}, z' = x' + y'\sqrt{3}i2$ and $x \equiv y, x' \equiv y' \mod 2$, we get $zz' = \frac{1}{4}(xx' - 3yy' + \sqrt{-3}(xy' + x'y))$ and checking the four

possibilities for the two mod two residues $x \equiv x', y \equiv y'$, we see the number in the denominator must be $\equiv 0 \mod 2$.

b. Let $\zeta := \exp(\frac{2\pi i}{6})$, also known as "the primitive sixth root of unity". (The Greek letter ζ is pronounced "zeta" and written "\zeta" in LaTeX). Show that $\zeta \in \mathbb{E}$ (in fact, you can observe that $\mathbb{E} = \{a + b\zeta \mid a, b \in \mathbb{Z}\}$). Show that $\zeta^6 = 1$, that $-\zeta = \zeta^4$ and $\bar{\zeta} = \zeta^{-1}$.

This can be done as a computation with complex numbers, or use trigonometry to see $\zeta = \exp(\pi i/3)$ so $\zeta^6 = \exp(2\pi i) = 1$ and $\zeta^4 = \zeta \cdot \exp(\pi i) = -\zeta$. And

$$\zeta^5 = \exp(\frac{5\pi i}{6}) = \exp(-\frac{\pi i}{6}) = \zeta^{-1} = \frac{\bar{\zeta}}{|\zeta|} = \frac{\bar{\zeta}}{1}.$$

c. Show that $C_1 \cap \mathbb{E} = \{1, \zeta, \zeta^2, \zeta^3, \zeta^4, \zeta^5\}$ is the set of the six distinct powers of ζ. (The notation C_r is, as before, the circle of radius r.)

Since $|\frac{x+iy\sqrt{3}}{2}| = \sqrt{\frac{x^2+3y^2}{4}}$, we see that the only possibilities for integer $|x|, |y|$ for which this is ≤ 1 are $|x| \leq 2, |y| \leq 1$. The only possibilities with $|x| \leq 1, |y| \leq 2$ and with the correct parity are $(|x|, |y|) = (0,0), (1,1), (2,0)$, and of these $(|x|, |y|) \in \{(2,0), (1,1)\}$ correspond to the correct parity. Putting in all possible signs we get $(x, y) \in (\pm 1, \pm 1)$, which corresponds to $z = \frac{\pm 1 \pm i \cdot \sqrt{3}}{2} = \{\sigma, \bar{\sigma}, -\sigma, -\bar{\sigma}$, and by the previous part this set is $\{\sigma, \sigma^2, \sigma^5, \sigma^4\}$. And the option $(x, y) = (\pm 2, 0)$ corresponds to $z = \pm 1 = \{\zeta^0, \zeta^3\}$. Thus $\zeta^0, \ldots, \zeta^5$ give the six distinct Eisenstein numbers of absolute value 1. And since $\zeta^5 = 1$, we have $\zeta^k = \zeta^{(k \mod 6)} \in \{\zeta^0, \ldots, \zeta^6\}$ for any integer k.

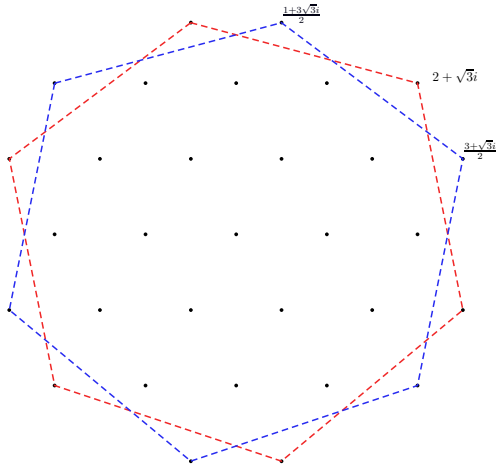
From now on, we write $U_6 := \{\zeta^k, 0 \leq k \leq 5\}$ for the set of unit Eisenstein numbers (here U_6 stands for "sixth roots of unity").

d. Show that if $z \in C_r$ (equivalently, $|z| = r$) then $\zeta^n z$ and $\bar{z}$ are also in C_r. Deduce that the set of Eisenstein integers in the circle C_r has number of elements divisible by 6.

Say $z \in C_r$. Then $|z| = r$, so $|z\zeta^n| = |z||\zeta^n| = |z| \cdot 1^n = r$, so $z\zeta^n \in C_r$. And $|\bar{z}| = r$ as well, so $\bar{z} \in C_r$. If z is an Eisenstein number then $\zeta^n z$ is also an Eisenstein number, as is $\bar{\zeta}$. Now let A_r be the set of Eisenstein numbers of radius r. It is finite since $|\frac{a+b\sqrt{3}i}{2}| = r$ implies $|a|, |b| \leq 2r$, and there are finitely many options for both a and b. Let A_r^k be the set of elements of A_r with argument in the interval $[k\pi, (k+1)\pi]$. Then $A_r^0, \ldots, A_r^5$ split up the set A_r into six "arcs". If $z \in A_r^k$ then $\zeta^{-k} z \in A_r^0$ and conversely for any $z \in A_r^0$, we have $\zeta^k z \in A_r^k$. Thus each of $A_r^0, A_r^1, \ldots, A_r^5$ has the same magnitude as A_r^0, and $|A_r| = 6|A_0|$. (Note: often, $|A_r|$ will be divisible by twelve, since for each $z \in A_r$ we can construct the six elements $\zeta^n z$ and six other elements $\zeta^n \bar{z}$. However, we are not guaranteed that these 12 elements are distinct! For example, we could have $\bar{z} = \zeta z$ or $\bar{z} = z$, etc. For a slightly more challenging exercise, prove that the number of points in A_r has number of points divisible by 12 if and only if r is not an integer or an integer times $\sqrt{3}$.

e. Find and draw twelve elements in $C_{\sqrt{7}} \cap \mathbb{E}$ (these are in fact all the

elements of $\mathbb{E}$ of length $\sqrt{7}$). Connect by a segment pairs of elements related by multiplication by ζ. (You should get two hexagons each consisting of groups of U_6-multiples!) See picture:



4. Fix a positive integer n. Let $z_{a,b} \in \mathbb{C}$ be an array of numbers indexed by pairs of integers a, b with $0 \leq a \leq n$ and $0 \leq b \leq n$ (you can think of this as an $n+1$ by $n+1$ square matrix, but thinking of $z_{a,b}$ as being in the point (a, b) of the plane rather than (b, a) as would be the case for matrix notation). Let $h_{a,b} := z_{a+1,b} - z_{a,b}$ for $0 \leq a \leq n-1, 0 \leq b \leq n$ be the matrix of horizontal differences (notice that $z_{a+1,b}$ only makes sense for $a \leq n-1$). Similarly, let $v_{a,b} := z_{a,b+1} - z_{a,b}$ for $0 \leq a \leq n$ and $0 \leq b \leq n-1$ be the matrix of vertical differences.

a. Show that for any pair of indices $a, b \in \{0, \ldots, n-1\}$ we have

$$v_{a,b} - v_{a+1,b} = h_{a,b} - h_{a,b+1} \tag{1}$$

It is helpful to think of the difference $v_{a,b}$ as corresponding to the vertical edge between the points (a, b) and $(a, b+1)$ and similarly for $h_{a,b}$ on a horizontal edge. This question is asking you to prove an identity about the numbers written on the edges of the little square connecting the four vertices $(a, b), (a+1, b), (a+1, b+1)$ and $(a, b+1)$.

The left hand side is $v_{a,b} - v_{a+1,b} = z_{a,b+1} - z_{a,b} - z_{a+1,b+1} + z_{a+1,b}$. The RHS is $z_{a+1,b} - z_{a,b} - z_{a+1,b+1} - z_{a,b+1}$, and the two are visibly equal.

b. Conversely, show that if we have collections of numbers $v_{a,b}$ (for $a \leq n, b \leq n-1$) and $h_{a,b}$ (for $a \leq n-1, b \leq n$) as above which satisfy equation (1) then there exists a collection of $z_{a,b}$ with $h_{a,b} = z_{a+1,b} - z_{a,b}$ and $v_{a,b} = z_{a,b+1} - z_{a,b}$, and that any two possibilities for the numbers $z_{a,b}$ differ from each other by a constant.

Hint: *Assume that $z_{0,0}$ is some constant number $c \in \mathbb{C}$. By considering the differences between consecutive pairs in the path $z_{0,0} \to z_{1,0} \to \cdots \to z_{a,0} \to$*

$z_{a,1} \to z_{a,2} \to \cdots \to z_{a,b}$, write a expression for $z_{a,b}$ in terms of $v_{j,k}$ and $h_{j,k}$. Now check that $h_{j,k}$ and $v_{j,k}$ are indeed the differences.

We will do a slightly different induction from the one described in the hint. Using the hint makes the induction argument simpler, but this one is more symmetric with respect to switching "vertical" and "horizontal" directions.

First, assume we are given some $h_{j,k}, v_{j,k}$ and $z_{j,k}$ is a collection of numbers satisfying $h_{j,k} = z_{j+1,k} - z_{j,k}$ and $v_{j,k} = z_{j,k+1} - z_{j,k}$. Then adding some constant $c \in \mathbb{C}$ to each $z_{j,k}$ will not change the differences. Other than adding a constant, there can be at most one set of values $z_{j,k}$ that works: indeed, once we know $c = z_{0,0}$ then we know $z_{1,0} = z_{0,0} + h_{0,0}$ and $z_{0,1} = z_{0,0} + v_{0,0}$. Now assume, by induction, that for some fixed $t \leq 2n$, we know each $z_{j,k}$ for $j + k \leq t$ (with the standing assumption $0 \leq j \leq n, 0 \leq k \leq n$). Then we know $z_{j+1,k} = z_{j,k} + h_{j,k}$ and $z_{j,k+1} = z_{j,k} + v_{j,k}$, and (by induction starting with the base case $t = 1$) this uniquely determines each value with $j + k = t + 1$.

This shows uniqueness up to constant, but we still need to show that at least one possibility for $z_{j,k}$ exists given that $h_{j,k}$ and $v_{j,k}$ satisfy property (1). To do this, it's enough to inductively construct $z_{j,k}$ for $j + k = t$ so that it satisfies $h_{j,k} = z_{j+1,k} - z_{j,k}$ and $v_{j,k} = z_{j,k+1} - z_{j,k}$ for $j + k < t - 1$. Assume (by the same kind of induction as above) that we have constructed $z_{j,k}$ for $j + k \leq t - 1$ that give the right $h_{j,k}$ and $v_{j,k}$ for $j + k < t - 2$. Now for $j + k = t$ satisfying $j \neq 0$ (so $k < t$) define $z_{j,k} = z_{j-1,k} + h_{j-1,k}$ and for $j + k = t$ satisfying $k \neq 0$, define $z'_{j,k} = z_{j,k-1} + v_{j,k-1}$. Now (applying the induction hypothesis) we have $z_{j,k} = z_{j-1,k} + h_{j-1,k} = (z_{j-1,k-1} + v_{j-1,k-1}) + h_{j-1,k}$ and $z'_{j,k} = z_{j,k-1} + v_{j,k-1} = z_{j-1,k-1} + h_{j-1,k-1} + v_{j,k-1}$. Since the h's and v's satisfy (1) we deduce $z'_{j,k} - z_{j-1,k-1} = z_{j,k} - z_{j-1,k-1}$ and so $z_{j,k} = z'_{j,k}$. Since $z_{j,k}$ was defined to have the right horizontal differences for $h_{j,k}$ (with $j + k = t - 1$) and $v_{j,k}$ was defined to have the right verticacl differences $v_{j,k}$ (for $j + k = t - 1$), we see that at the t'th inductive step, the $z_{j,k}$ have the correct differences for all adjacent pairs with sum of indices $\leq t$. At the $2n$th step of the induction, we will have thus constructed the values $z_{j,k}$ (with $0 \leq j \leq n, 0 \leq k \leq n$) with the desired properties.

c. Let $\lambda_h, \lambda_v \in \mathbb{C}$ be two arbitrary complex numbers. Define arrays

$$h_{a,b} := \lambda_h \cdot (a + bi)$$

and

$$v_{a,b} := \lambda_v \cdot (a + bi).$$

Show that equation (1) is satisfied (so these particular choices $h_{a,b}, v_{a,b}$ are indeed differences) of and only if $\lambda_v = i \cdot \lambda_h$.

We check (1): We want $h_{a-1,b} - h_{a-1,b-1} = v_{a,b-1} - v_{a-1,b-1}$. Putting in the given values of $h_{a,b}$ and $v_{a,b}$ we get the left hand side equal to $\lambda_h \left((a-1) + bi - (a - 1 + (b-1)i)\right) = \lambda_h \cdot i$ and teh right hand side is $\lambda_v \left(a + (b-1)i - (a - 1 + (b-1)i)\right) = \lambda_v$, so the condition holds if and only if $\lambda_v = i\lambda_h$.

Notice the similarity between the condition $\lambda_v = i \cdot \lambda_h$ and complex differentiability. A continuous version of this type of argument (with $z_{a,b} := f(\frac{a+bi}{n})$,

and with n approaching ∞) is useful for proving integration and differentiation formulas for holomorphic functions.