M4P58 DISCUSSION PROBLEMS 1

These problems are for discussion in lecture and will NOT be assessed. They are somewhat more difficult than typical assessed coursework problems; do not get discouraged if it is not immediately clear how to approach them. Working on these in groups with your fellow students and trading ideas and approaches is HIGHLY encouraged!

If you have difficulty getting complete solutions to any particular problem it might be helpful to: work out some examples, try to find partial results in special cases, identify related, easier questions, etc. If all else fails, I am happy to give hints in office hours!

1. Let V be a finite dimensional real vector space, and recall that a lattice in V is a closed discrete additive subgroup of V that spans V over $\mathbb{R}$. Show that every lattice in V has the form $\mathbb{Z} \cdot v_1 + \mathbb{Z} \cdot v_2 + \cdots + \mathbb{Z} \cdot v_n$ for some basis $v_1, \dots v_n$ of V. (In particular, the lattices in $\mathbb{C}$ have the form claimed in lecture.) [Hint: first show that such a lattice is a finitely generated abelian group. You will then need the fact that a finitely generated abelian group with no elements of finite order is isomorphic to $\mathbb{Z}^r$ for some r.]

2. Let L be a lattice in $\mathbb{C}$. and denote by $\mathrm{End}(L)$ the subring of $\mathbb{C}$ consisting of $z \in \mathbb{C}$ such that $zL \subseteq L$. Let $\mathrm{Aut}(L)$ be the group $\mathrm{End}(L)^{\times}$; this is the subgroup of $\mathbb{C}^{\times}$ consisting of z such that $zL = L$.

2a. Show that either $\mathrm{End}(L) = \mathbb{Z}$ or $\mathrm{End}(L) = \mathbb{Z}[\alpha]$ for some $\alpha \in \mathbb{C} \setminus \mathbb{R}$ satisfying a polynomial of the form $\alpha^2 + a\alpha + b$, for $a, b \in \mathbb{Z}$. In the latter case we say that L "has complex multiplication by $\mathbb{Z}[\alpha]$".

2b. Show that if L has complex multiplication by $\mathbb{Z}[\alpha]$ then there exists $z \in \mathbb{C}$ such that zL is an ideal of $\mathbb{Z}[\alpha]$. Conversely, show that if $z \in \mathbb{C}$ and L is an ideal of $\mathbb{Z}[\alpha]$, then L has complex multiplication by a ring containing $\mathbb{Z}[\alpha]$, and contained in $\mathbb{Q}[\alpha]$.

2c. Show that if $\mathrm{Aut}(L)$ is not ± 1, then, up to homothety, $L = L_{i,1}$ or $L_{\rho,1}$, where $\rho = e^{\frac{2\pi i}{3}}$.

3. Show, using the q-expansions for E_4 and E_6, and the formula $\Delta = \frac{E_4^3 - E_6^2}{1728}$, that the q-expansion of Δ has integral coefficients.

4. Recall that the Bernoulli numbers b_k were defined by the identity:

$$\frac{x}{e^x - 1} = \sum_{k=0}^{\infty} \frac{b_k}{k!} x^n.$$

4a. Show that the b_k may be defined recursively by the equations:

- $b_0 = 1$
- For all $m \geq 1$, $b_m = -\frac{1}{m+1} \sum_{k=0}^{m-1} \binom{m+1}{k} b_k$.

4b. For any positive integers n, m, let $S_m(n)$ denote the sum $1^m + 2^m + \cdots + (n-1)^m$. Show that one has:

$$S_m(n) = \frac{1}{m+1} \sum_{k=0}^{m} \binom{m+1}{k} b_k n^{m+1-k}.$$

(This was Bernoulli's original motivation for studying what eventually became known as the Bernoulli numbers.)