Algebra, Number Theory and Combinatorics (Overall individual round, 2021)

Problem 1. (Overall individual round). For any $n \geq 1$, let A denote the \mathbb{C} algebra consisting of $n \times n$ upper triangular complex matrices $\left\{\begin{pmatrix} * & * & * \\ 0 & * & * \\ 0 & 0 & * \end{pmatrix}\right\}$.

We shall consider the left A-modules (that is, \mathbb{C} -vector spaces V with \mathbb{C} -algebra

We shall consider the left A-modules (that is, \mathbb{C} -vector spaces V with \mathbb{C} -algebra homomorphisms $\rho: A \to \operatorname{End}(V)$).

- (1) Show that all simple modules of A are finite dimensional.
- (2) Determine all simple modules of A.

Problem 2. (Overall individual round). Let p be a prime number. Prove the following theorem of Euler: the equation $p = x^2 + 3y^2$ has a solution with $x, y \in \mathbb{Z}$ if and only if p = 3 or $p \equiv 1 \pmod{3}$. (You may use the fact that the ring of integers of $\mathbb{Q}(\sqrt{-3})$ is a principal ideal domain.)

Solution to Problem 1 (Overall individual round). (1) Let E_{ij} denote the matrix whose (i, j)-entry is 1 and other entries vanish. Then E_{ij} , $i \leq j$, form a basis of A. In particular, A is finite dimensional.

Let V denote a non-zero module. Take any $0 \neq v \in V$. Then Av is a non-zero submodule of V. And Av is finite dimensional because A is. Since V is simple, V = Av is finite dimensional.

- (2a) Let S_i , $1 \le i \le n$, denote the 1-dimensional modules such that E_{ii} acts by 1 and E_{ij} , E_{jj} acts by 0 for $j \ne i$. They are simple modules.
- (2b) It remains to show that the S_i we have constructed are the only simple modules. Let S denote any finite dimensional simple module.

We claim that E_{ij} , i < j, form a nilpotent 2-sided ideal N (because the product of an upper triangular matrix with a strictly upper one is strictly upper).

Then N acts on S by 0 (To see this, NS is a submodule of S. It is proper because N is nilpotent. Since S is simple, we deduce that NS = 0.)

Note that the action of E_{ii} commute with each other (and with the 0-action by E_{ij}), thus they are module endomorphisms. By Schur's Lemma, E_{ii} acts on S as a scalar. Since $E_{ii}E_{jj}=0$ for $i\neq j$, at most one E_{ii} acts as a non-zero scalar. Recall that $1=\sum_i E_{ii}$ acts by the identity. The claim follows.

Solution to Problem 2 (Overall individual round). The "only if" part is clear. We prove the "if" part. For p=3 one can take (x,y)=(0,1). Assume $p\equiv 1\pmod 3$. By quadratic reciprocity, $(\frac{-3}{p})=(\frac{p}{3})=1$. Thus p splits in $\mathbb{Q}(\sqrt{-3})$. The ring of integers of $\mathbb{Q}(\sqrt{-3})$ is $\mathbb{Z}[\omega]$, where $\omega=\frac{-1+\sqrt{-3}}{2}$. Since $\mathbb{Z}[\omega]$ is a PID, there exists $\pi\in\mathbb{Z}[\omega]$ such that $N_{\mathbb{Q}(\sqrt{-3})/\mathbb{Q}}(\pi)=p$. We claim that at least one of π , $\pi\omega$, and $\pi\omega^2$ belongs to $\mathbb{Z}[\sqrt{-3}]$ and thus is of the form $x+y\sqrt{-3}$ with $x,y\in\mathbb{Z}$. Taking norms, we then get $p=x^2+3y^2$.

To prove the claim, we may assume $\pi = \frac{a+b\sqrt{-3}}{2}$, where a and b are odd integers. Then either $4 \mid a - b$ (which is equivalent to $\pi\omega \in \mathbb{Z}[\sqrt{-3}]$) or $4 \mid a + b$ (which is equivalent to $\pi\omega^2 \in \mathbb{Z}[\sqrt{-3}]$).