GRV II test 2a.

1. The map $\phi : \mathbb{Z}^3 \to \mathbb{Z}^3$ is given by the matrix

$$A := \begin{pmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \\ 7 & 8 & 9 \end{pmatrix}$$

   (a) Compute the standard form of the $\mathbb{Z}$-module $\mathbb{Z}^3/\mathrm{im}(\phi)$.

   Using elementary row and column operations (switching columns or rows, multiplying columns or rows by units (i.e. ± 1), and replacing a column resp. row by the sum of that column resp. row minus an integer-multiple of another column resp. row) we end up with a diagonal matrix, with $1, 3, 0$ on the diagonal. So our module is then $\mathbb{Z}/(1) \oplus \mathbb{Z}/(3) \oplus \mathbb{Z}/(0) \cong \mathbb{Z} \oplus \mathbb{Z}/(3)$.

   - Rank: 1
   - Invariant factor(s): 3.

     If you wrote rank = 1 and invariant factors = 1,3 then that corresponds to the same module.
     It is standard practice to deleting units from the invariant factors; this does not change the module as it corresponds to deleting trivial $\mathbb{Z}/(1)$'s.

   (b) What is the minimal number of generators for $\mathbb{Z}^3/\mathrm{im}(\phi)$?

   Answer: 2. The module is not cyclic, so 1 won't do, and clearly $\{(1, 0), (0, 1)\}$ generates $\mathbb{Z} \oplus \mathbb{Z}/(3)$.

2. Up to similarity, how many 4 by 4 matrices over $\mathbb{F}_p$ exist whose characteristic polynomial is not equal to its minimal polynomial?

   The invariant factors are monic polynomials with $a_1|a_2|\cdots|a_m$. Here $m > 1$ since the minimal polynomial (which equals a_m) must differ from the characteristic polynomial (which equals $a_1 \cdots a_m$). The degrees must be a non-decreasing sequence with m entries adding up to 4:

   $2 + 2$: $a_1 = a_2 =$ any monic polynomial of degree 2 (there are p^2 such polynomials).
   $1 + 3$: $a_1 =$ monic and linear (p cases) and a_2/a_1 is monic quadratic (p^2 cases, for a total of $p \cdot p^2$ cases).
   $1 + 1 + 2$: $a_1 = a_2$ is linear and a_3/a_2 is linear for a total of $p \cdot p$ cases.
   $1 + 1 + 1 + 1$: $a_1 = \cdots = a_4$ is linear, p cases.

   Total: $p^2 + p^3 + p^2 + p = p^3 + 2p^2 + p$.

3. Let A be an n by n matrix over $\mathbb{Q}$. If all eigenvalues are in $\mathbb{Q}$ then show that there exists a basis $b_1, \ldots, b_n$ of $\mathbb{Q}^n$ for which $Ab_1 \in \mathrm{SPAN}_{\mathbb{Q}}(b_1)$ and $Ab_i \in \mathrm{SPAN}_{\mathbb{Q}}(b_i, b_{i-1})$ for $i = 2, \ldots, n$.

All eigenvalues are in $\mathbb{Q}$ so A is similar (over $\mathbb{Q}$) to a matrix J in Jordan Normal Form. This matrix J only has entries on the diagonal and on the line directly above the diagonal, in other words, $Je_1 \in \text{SPAN}_{\mathbb{Q}}(e_1)$ and $Je_i \in \text{SPAN}_{\mathbb{Q}}(e_i, e_{i-1})$ for $i > 1$. The fact that J is similar to A means that there is some basis $b_1, \ldots, b_n$ such that the matrix of the linear map $v \mapsto Av$ with respect to basis $b_1, \ldots, b_n$ is J. For that basis we have the required property.

4. Let m be a positive integer and $f = x^m - 2$. Show that f is irreducible. If A is an n by n matrix over $\mathbb{Q}$ and $A^m = 2I$ then show that $m|n$.

   f is 2-Eisenstein and hence irreducible in $\mathbb{Z}[x]$ (and thus irreducible in $\mathbb{Q}[x]$ by Gauss' lemma).

   Since $f(A) = 0$ it follows that f is divisible by the minimal polynomial of A. But f is irreducible so f equals the minimal polynomial. The characteristic polynomial divides a power of the minimal polynomial, so it divides a power of f. But if $g|f^N$ and g is monic, and f is irreducible, then g must also be a power of f. So the characteristic polynomial is a power of f. So its degree (which equals n) must be divisible by the degree of f (which equals m).

5. (bonus or take-home) (if exercises 1–4 are correct then you aced the test).

   Let R be a PID and let M be a finitely generated R-module with annihilator $(f) \neq (0)$. Show that there exists a homomorphism $\phi : M \to M$ with $\phi \circ \phi = \phi$ and $\phi(M) \cong R/(f)$.

   By the classification theorem, we may (up to isomorphism) write M as $R/(a_1) \oplus \cdots \oplus R/(a_m)$ with $a_m = f$. Now let $\phi : R/(a_1) \oplus \cdots \oplus R/(a_m) \to R/(a_1) \oplus \cdots \oplus R/(a_m)$ send $(r_1, \ldots, r_m)$ to $(0, \ldots, 0, r_m)$. Then $\phi \circ \phi = \phi$ and $\phi(M) = \{0\} \oplus \cdots \oplus \{0\} \oplus R/(a_m) \cong R/(a_m) = R/(f)$.