PROJECT GROUP 3 – FOOD FOR THOUGHT

Please report all typos, errors and nonsensical statements!

(1) Let L be the splitting field of the polynomial $f(X) = X^3 - 2X + 1$. What is the smallest conductor of an elliptic curve $E/\mathbf{Q}$ with $\mathbf{Q}(E[2]) = K$?

(2) Look up the Bordeaux tables of cubic fields. For the 10 cubic fields K of smallest discriminant, find the smallest conductor of an elliptic curve $E/\mathbf{Q}$ such that $\mathbf{Q}(E[2])$ is equal to the Galois closure L of K.

(3) Find an elliptic curve $E/\mathbf{Q}$ such that $\mathbf{Q}(E[3])$ is equal to the splitting field of $f(X) = X^4 - 44X^2 + 528$.

(4) Let G be a closed subgroup of $\mathbf{GL}_2(\mathbf{Z}_p)$ with $p \geq 5$. Suppose the image $\overline{G}$ of G in $\mathbf{GL}_2(\mathbf{F}_p)$ contains $\mathbf{SL}_2(\mathbf{F}_p)$. Show that G contains $\mathbf{SL}_2(\mathbf{Z}_p)$.[1]

(5) Find a proper subgroup G of $\mathbf{SL}_2(\mathbf{Z}/9\mathbf{Z})$ which maps isomorphically onto $\mathbf{SL}_2(\mathbf{Z}/3\mathbf{Z})$ under the reduction map. Suppose G is a subgroup of $\mathbf{SL}_2(\mathbf{Z}/9\mathbf{Z})$ that surjects onto $\mathbf{SL}_2(\mathbf{Z}/3\mathbf{Z})$. Show that $G = \mathbf{SL}_2(\mathbf{Z}/9\mathbf{Z})$ or the surjection from G onto $\mathbf{SL}_2(\mathbf{Z}/3\mathbf{Z})$ is an isomorphism. How many conjugacy classes of $\mathbf{SL}_2(\mathbf{Z}/3\mathbf{Z})$s are there in $\mathbf{SL}_2(\mathbf{Z}/9\mathbf{Z})$? Same question with $\mathbf{SL}_2$ replaced by $\mathbf{PSL}_2$. Can you find some elliptic curves such that the image of $\overline{\rho}_{E,3}$ is equal to G?[2]

(6) If $G \subset \mathbf{SL}_2(\mathbf{Z}/4\mathbf{Z})$ and $\overline{G} = \mathbf{SL}_2(\mathbf{Z}/2\mathbf{Z})$, then $|G| = 12$ or 48. If $G \subset \mathbf{SL}_2(\mathbf{Z}/8\mathbf{Z})$ and $\overline{G} = \mathbf{SL}_2(\mathbf{Z}/2\mathbf{Z})$, then $|G| = 12$, 24, 48, 96, or 384. Except for 384, all of these possibilities occur with G not surjecting onto $\mathbf{SL}_2(\mathbf{Z}/4\mathbf{Z})$. Discuss conjugacy of these groups in $\mathbf{SL}_2$ and $\mathbf{PSL}_2$? Can you find some elliptic curves such that the image of $\overline{\rho}_{E,8}$ is equal to G?[3]

(7) Having played with the last two problems, do you have any thoughts or feedback about Sage's capacity for computing with finite groups like $\mathbf{GL}_2(\mathbf{Z}/p^n\mathbf{Z})$, $\mathbf{SL}_2(\mathbf{Z}/p^n\mathbf{Z})$ and $\mathbf{PSL}_2(\mathbf{Z}/p^n\mathbf{Z})$.

(8) Suppose $E/\mathbf{Q}$ admits a rational p-isogeny, so that the mod p representation is reducible:
$$\overline{\rho}_{E,p}(\sigma) \sim \begin{pmatrix} \epsilon(\sigma) & * \\ 0 & \epsilon(\sigma)^{-1}\omega(\sigma) \end{pmatrix}$$
Can we compute anything about the character ϵ? Its order? Its conductor?

Date: June 21, 2010.

[1] You can look in Serre's 1972 Inventiones paper *Propriétés galoisiennes des points d'ordre fini des courbes elliptiques* for hints.

[2] Elkies has shown how to parametrize these curves. See `http://arxiv.org/abs/math/0612734`.

[3] We should study Elkies' paper and see if we can provide a similar parametrization here.