1 Projects

Project 1 (Endomorphisms of hyperelliptic Jacobians)**.** Zarhin has proven [Zar00] the following remarkable theorem:

Theorem 1 (Zarhin)**.** *Let $f(x)$ be a separable polynomial of degree $n \geq 5$ with coefficients in a number field K. Let C be the hyperelliptic curve $y^2 = f(x)$, and suppose that the Galois group of $f(x)$ over K is either A_n or S_n. Then for the Jacobian J of C we have* $\mathrm{End}_{\overline{K}}(J) = \mathbb{Z}$.

The aim of this project is to find similar criteria which give information on $\mathrm{End}_{\overline{K}}(J)$ (or $\mathrm{End}_K(J)$) in terms of properties of the Galois group G of $f(x)$: here are two possible extensions for you to think about.

1. are there assumptions on G (weaker than G containing A_n, of course) that ensure that J is geometrically irreducible?

2. fix a (small) value of g and a proper subgroup H of A_n. Is there a polynomial $f_H(x)$ of degree n with Galois group H and such that the Jacobian J_H of $y^2 = f_H(x)$ has (geometrically) nontrivial endomorphism ring? If the answer is yes, then you have found an abelian variety with an 'interesting' Galois representation (nontrivial endomorphisms and prescribed structure on $J_H[2]$). If the answer is no, you have found a strengthening of Zarhin's theorem.

Project 2 (Small torsion of non-hyperelliptic Jacobians)**.** The purpose of this exercise is to investigate the geometry of torsion points of small order on Jacobians of non-hyperelliptic curves.

1. Let C be a genus-3 non hyperelliptic curve, presented as a smooth plane quartic $F(X, Y, Z) = 0$. Can you describe the 2-torsion in $J = \mathrm{Jac}(C)$ in terms of the geometry of F? [This is known, but still interesting].

2. Can you find a similar geometric description for a non-hyperelliptic genus 4 curve presented as the intersection of a quadric and a cubic in $\mathbb{P}^3$?

3. Can you find further interesting classes of curves C for which some of the groups $\mathrm{Jac}(C)[\ell]$ are easy to describe in geometric terms?

Project 3 (A surjectivity criterion in genus 2)**.** As described in Sara's lectures on elliptic curves, there is a surjectivity criterion for Galois representations attached to elliptic curves (due to Serre) which reads as follows:

Theorem 2 (Serre)**.** *Let E be an elliptic curve over a number field K. Let $p \geq 5$ be a prime number and let G_p be the image of the representation ρ_p attached to E. Suppose that G_p contains:*

1. *an element g such that $\mathrm{tr}(g) \neq 0$ and $\mathrm{tr}(g)^2 - 4\det(g)$ is a nonzero square in $\mathbb{F}_p^\times$*

2. *an element* g' *such that* $\mathrm{tr}(g') \neq 0$ *and* $\mathrm{tr}(g')^2 - 4\det(g')$ *is not a square in* $\mathbb{F}_p^\times$

3. *an element* g'' *such that* $u := \mathrm{tr}(g'')^2/\det(g'')$ *satisfies* $u \neq 0, 1, 2, 4$ *and* $u^2 - 3u + 1 \neq 0$

Then G_p *contains* $\mathrm{SL}_2(\mathbb{F}_p)$*. In particular, if* p *is unramified in* K*, then* $G_p = \mathrm{GL}_2(\mathbb{F}_p)$*.*

Can you find a similar criterion for abelian surfaces (the classification of proper subgroups of $\mathrm{GSp}_4(\mathbb{F}_\ell)$ given in [Lom16] might be useful)?

Project 4 (Prime values of some quadratic polynomials)**.** Consider the elliptic curve $E : y^2 = x^3 + x$ over the field $\mathbb{Q}$. Let $p \equiv 1 \pmod 4$ be a prime number; it is well-known that p can be written as $p = a^2 + b^2$ in an essentially unique[1] way.

1. Compute the trace of the Frobenius at p in terms of a and b.

2. Notice that whenever the trace of the Frobenius at p is ± 2 the prime number p is of the form $x^2 + 1$ (and recall that it is not known whether there exist infinitely many primes of this form).

3. Google the Lang-Trotter conjecture (a good reference for the purposes of this project is [BJ09]). Combined with the previous remarks, what does the Lang-Trotter conjecture imply on the distribution of primes p of the form $x^2 + 1$?

4. Can you derive the same prediction from analytic number theory, without resorting to the theory of elliptic curves?

5. Apply the same argument to other CM elliptic curves over $\mathbb{Q}$. What are the corresponding predictions about the prime values taken by certain quadratic polynomials?

6. Can you support these predictions by analytic arguments and/or with numerical experiments?

7. ($\star$) Can you find a higher-dimensional analogue of these heuristics? (That is, can you make similar predictions by looking at CM abelian varieties of dimension 2 or more?)

References

[BJ09] Stephan Baier and Nathan Jones. A refined version of the Lang-Trotter conjecture. *Int. Math. Res. Not. IMRN*, (3):433–461, 2009.

[Lom16] D. Lombardo. Explicit surjectivity for Galois representations attached to abelian surfaces and GL_2-varieties. *Journal of Algebra*, 460C:26–59, 2016.

[Zar00] Yu. G. Zarhin. Hyperelliptic Jacobians without complex multiplication. *Math. Res. Lett.*, 7(1):123–132, 2000.

[1] that is, up to exchanging a and b and to a choice of signs