ARITHMETIC ASPECTS OF EXPLICIT MODULI PROBLEMS
PROBLEM SESSION

Problem 1 (David Zureick–Brown). Compute $X_H(\mathbb{Q})$ from the following list of curves.

```
P2<x,y,z> := ProjectiveSpace(Rationals(),2);

// level 3^n curves
X33:= Curve(P2, -x^3*y + x^2*y^2 - x*y^3 + 3*x*z^3 + 3*y*z^3);
X43:= Curve(P2, x^3*z - 6*x^2*z^2 + 3*x*y^3 + 3*x*z^3 + z^4);

// level 5^n curves
R<x> := PolynomialRing(Rationals());
S<a,b,c,d> := PolynomialRing(Rationals(),4);

h := x^3 + x + 1;
f := 6*x^6 + 5*x^5 + 12*x^4 + 12*x^3 + 6*x^2 + 12*x - 4;
X11 := HyperellipticCurve([f,h]);

h2 := x^3 + x + 1;
f2 := x^6 - 13*x^4 - 38*x^3 + 6*x^2 + 22*x + 6;
X15 := HyperellipticCurve([f2,h2]);

f1 := a^2 + 51*a*b + 648*b^2 - 900*a*c - 22086*b*c + 211572*c^2 - 25650*a*d
      - 629856*b*d + 11499732*c*d + 156402576*d^2;
f2 := a*b^2 + 24*b^3 - 438*a*b*c - 10818*b^2*c - 11232*a*c^2 -  186732*b*c^2
      - 243648*c^3 - 12996*a*b*d - 320382*b^2*d -  285444*a*c*d - 2161728*b*c*d
      - 104818536*c^2*d +  992412*a*d^2 + 90530136*b*d^2 - 5156170344*c*d^2
      - 67660478712*d^3;
X16 := Curve(ProjectiveSpace(Rationals(),3),[f1,f2]);
```

Problem 2 (David Zureick–Brown). In Theorem 1.4 of Várilly-Alvarado–Viray

`https://sites.math.washington.edu/~bviray/papers/VAV_UniformBoundRank19K3.pdf`

and degree $r'' = 2$ (so over quadratic fields), apply results of Bruin–Najman

`https://arxiv.org/pdf/1406.0655.pdf`

so with finitely many exceptions, an elliptic curve over a quadratic extension with a cyclic n-isogeny is a $\mathbb{Q}$-curve.

Problem 3 (Eric Katz). A question related to the Chabauty method: define iterated p-adic integrals in a down-to-earth way without using Frobenius. Suppose C over $\mathbb{Q}_p$ has good reduction. Classically, a p-adic integral comes about via

$$C(\mathbb{C}_p) \hookrightarrow J(\mathbb{C}_p) \xrightarrow{\text{Log}} \text{Lie}\, J(\mathbb{C}_p);$$

Date: June 7, 2017.

so for iterated integrals, we need to replace J by a unipotent analogue.

Problem 4 (René Schoof). Let X be a nice curve over $\mathbb{Q}$ of genus $g \geq 1$ given by equations in projective space $\mathbb{P}^n$ equipped with a height function h. Let $P_0 \in X(\mathbb{Q})$, and use P_0 to embed $X(\mathbb{Q}) \hookrightarrow J(\mathbb{Q})$ by $P \mapsto [P - P_0]$. One has the canonical height $\widehat{h}$ on $J(\mathbb{Q})$. Are there bounds for $h(P)$ in terms of $\widehat{h}([P - P_0])$? If $g = 1$, there are bounds in Silverman. (We would use this to say that points in a box on $J(\mathbb{Q})$ determine points in a box on $X(\mathbb{Q})$.)

Problem 5 (Kiran Kedlaya). By an old result of Mumford, the closure of the moduli space of principally polarized abelian fourfolds with trivial geometric endomorphism algebra but the MumfordTate group is nontrivial ($\mathrm{SL}_2 \times \mathrm{SL}_2 \times \mathrm{SL}_2$) is nonempty and a countable union of components of dimension 1.

(a) Give an explicit model for one or more components.
(b) Give explicit points, especially on the Torelli locus.
(c) For points on the Torelli locus, what fields of definition are possible? (Is it possible to show or rule out the existence of an example over $\mathbb{Q}$?)

Problem 6 (Jeroen Sijsling). As in Problem 5, let X be a nice curve over $\mathbb{Q}$ of genus $g \geq 1$ given by equations in $\mathbb{P}^n$. Embed $X(\mathbb{Q}) \hookrightarrow J(\mathbb{Q})$ by $P \mapsto [P - P_0]$ for $P_0 \in X(\mathbb{Q})$.

Now let $M : H^0(X, \omega_X) \to H^0(X, \omega_X)$ be a matrix representing a candidate endomorphism α of J. To check if α is an endomorphism, we compute

$$\alpha([P - P_0]) = \sum_{i=1}^{g} [Q_i - P_0]$$

and make the corresponding graph $Y \subset X \times X$, the closure of the points (P, Q_i) so obtained.

(a) The projection onto the first component is degree g. What is the degree of the projection onto the second projection?
(b) Which monomials are needed to define $Y \subseteq \mathbb{P}^n \times \mathbb{P}^n$, i.e., those monomials in some set of generators for the ideal of vanishing of Y?
(c) What can one say about the sizes of the coefficients in the equations defining Y?

Problem 7 (Maarten Derickx). Derickx–Kamienny–Mazur

`http://www.math.harvard.edu/~mazur/papers/For.Momose20.pdf`

prove that every point on $X_1(17)$ defined over a quartic field comes from a rational function of degree 4 on $X_1(17)$; moreover, up to $(\mathbb{Z}/17\mathbb{Z})^*/\{\pm 1\}$, there are three such functions, with Galois group once S_4 and twice D_4. Note there exists an elliptic curve E over a number field K with $\mathrm{Gal}(K/\mathbb{Q}) \simeq C_4$ cyclic which has a direct explanation.

Find the rational points on those curves that classify when the Galois group of these points is smaller: for the normal closure $X \to X_1(17) \to \mathbb{P}^1$ and a subgroup $H \leq \mathrm{Gal}(X/\mathbb{P}^1)$, we find modular curves $X/H \to \mathbb{P}^1$ and there are six left.

For more detail, see the file

`http://www.birs.ca/workshops/2017/17w5065/files/X_1(17)_D4_S4.txt`

Problem 8 (Jennifer Johnson–Leung). Let F be a Siegel paramodular form of level N with Fourier–Jacobi expansion

$$F(\tau, \tau', z) = \sum_k f_k(\tau, z) q^k.$$

Let χ be a quadratic character of conductor p, and consider the twist

$$F(\tau, \tau', z; \chi) = \sum_k \chi(k) f_k(\tau, z) q^k;$$

the twist is no longer a Siegel paramodular form, but rather, it is stable under the *stable paramodular group* $K_s(p^n) = K(p^n) \cap K(p^{n-1})$ where $p^n \parallel N$ and $K(m)$ is the paramodular group of level m. The representation theory of the group $K_s(p^n)$ is very nice, worked out by Ralf Schmidt, with newspaces of dimension 1 when they are supposed to be—and there are Hecke operators.

Is there a geometric object associated to $F(\tau, \tau', z; \chi)$? And is there some class of abelian surfaces for which the Galois representations coincide?

Problem 9 (Bjorn Poonen). Let $p > 2$ be a prime, let $k = \mathbb{F}_p(t)$ and $X : y^p = tx^p + x$. Compute $X(k)$. Is there a nice way to do it?

This curve is smooth and has the structure of an additive group. But over a base extension, the genus goes down, and by work of Voloch the set of points is finite, so the answer is a finite abelian group. (For $p = 2$, the curve is a conic birational to $\mathbb{P}^1$.)

Several people suggested an argument to prove that $(0, 0)$ is the only solution. In particular, Bas Edixhoven used a parametrization of the curve over $\mathbb{F}_p(u)$ with $u^p = t$, and then imposed the conditions that dx/du and dy/du be zero to ensure that x and y are in $\mathbb{F}_p(t)$ instead of just $\mathbb{F}_p(u)$.

Problem 10 (Drew Sutherland). Given a smooth plane quartic X over $\mathbb{Q}$ compute $\mathrm{Jac}(X)(\mathbb{Q})_{\mathrm{tors}}$ efficiently. This would be useful for the database of genus 3 curves going into the LMFDB.

For hyperelliptic of genus 3, in principle it has been worked out. Work modulo many primes to get an upper bound and look for rational points to match. Perhaps Chaubauty's method works (make Manin–Mumford effective)? Perhaps a Hensel lifting method works?

(It may also be interesting to work out the geometrically hyperelliptic but non-hyperelliptic curves.)

Problem 11 (Elisa Lorenzo Garcia). What modular curves $X(\Gamma)$ have a smooth plane model? (In particular, all genus three *non*-hyperelliptic modular curves.) Then $g = (d-1)(d-2)/2$ for a degree d, and we need a g^2_d-linear system on X. Such a curve has gonality $\sqrt{g}$, so using an effective bound on the gonality this should reduce the problem to a finite list?

Problem 12 (David Zureick–Brown). Is there a surface S which is *not* the quotient of the product of two curves, with a nontrivial Albanese variety, such that one can apply Chabauty's method?

Problem 13 (Armand Brumer). We leave it to the reader to generalize this in the obvious manner. It is motivated by making sure that we might someday be able to find all abelian surfaces over $\mathbb{Q}$ of given conductor.

Let S be a finite set of primes, $\mathcal{A}(S)$ be the finite set of abelian surfaces good outside S, and $\mathcal{J}(S)$ the set of Jacobians in $\mathcal{A}(S)$. Introduce an invariant $d(S)$ and a set $T(S)$ as follows. For each isogeny class in $\mathcal{A}(S)$, take the minimum degree of any polarization and then let $d(S)$ be the

maximum over the isogeny classes in $\mathcal{A}(S)$. Let $T(S)$ be a minimal set of places such that each isogeny class in $\mathcal{J}(S)$ contains a Jacobian $\mathrm{Jac}(C)$ such that C is good outside $T(S)$.

What can be said about $d(S)$ and $T(S)$. Is $d(S)$ bounded as S grows?

Even 30 years after Faltings, the only case understood is $S = \emptyset$! Even for $S = \{2\}$ neither $d(S)$ nor $T(S)$ are known. The work of Merriman–Smart only find the curves good outside 2, but there are many other examples beyond this list.

The problem is slightly easier if one restricts to semistable abelian varieties: for a few sets S, one may find all semistable surfaces good outside S, up to isogeny, thanks to Schoof or Brumer–Kramer.

Problem 14 (Samuele Anni). Let $E/\mathbb{Q} : y^2 + y = x^3 - x$ (LMFDB label 37.a1). For every prime ℓ we have that $\mathrm{Gal}(\mathbb{Q}(E[\ell])/\mathbb{Q}) \cong \mathrm{GL}_2(\mathbb{F}_\ell)$. This gives a realization of $\mathrm{GL}_2(\mathbb{F}_\ell)$ as Galois group over $\mathbb{Q}$ for all primes ℓ using "one object". Is there an analogous construction, i.e. simultaneous realization of $\mathrm{GL}_2(\mathbb{F}_\ell)$ for all ℓ as Galois group using the "same object", over any number field different from $\mathbb{Q}$?

Problem 15 (John Voight). Computations with paramodular forms and L-functions suggest that there is an abelian surface A over $\mathbb{Q}$ of conductor 550 whose first few Euler factors (computed by David Farmer and Sally Koutsoliotas, the first few by Cris Poor and David Yuen) are as follows:

$$\begin{aligned} L_2(T) &= (1+T)(1+2T^2) \\ L_3(T) &= 1 - T^2 + 9T^4 \\ L_5(T) &= 1 + 3T + 5T^2 \\ L_7(T) &= 1 + 4T^2 + 49T^4 \\ L_{11}(T) &= (1+T)(1-3T+11T^2) \\ L_{13}(T) &= 1 - 8T^2 + 169T^4 \end{aligned}$$

Show that such a surface exists! Because $L_3(T)$ is irreducible, if A exists then A is simple over $\mathbb{Q}$. The abelian surface A may or may not have a principal polarization over $\mathbb{Q}$. We expect that $A[2]$ is extension of $E_1[2]$ by $E_2[2]$, where E_i are elliptic curves of conductor 11 and 50 respectively. The first few Dirichlet coefficients of the L-function are:

$$\begin{aligned} \{&1,-1,0,-1,-3,0,0,1,1,3,2,0,0,0,0,3,-3,-1,1,3,0,-2,-3,0,4,0,0,0,0,0,-5,-3,0,3,0,-1,\\ &3,-1,0,-3,-3,0,12,-2,-3,3,6,0,-4,-4,0,0,-6,0,-6,0,0,0,3,0,-14,5,0,-5,0,0,0,\\ &3,0,0,3,1,-3,-3,0,-1,0,0,10,-9,-8,3,-3,0,9,-12,0,2,0,3,0,3,0,-6,-3,0,9,4,2,-4,12,\\ &0,6,0,0,6,21,0,4,6,0,0,0,0,9,0,0,-3,0,0,-4,14,0,5,3,0,-18,5,0,0,0,0,0,0,0,-3,-6,0,1,\\ &0,0,-3,0,3,0,3,0,-3,-6,0,-8,1,-3,0,15,0,-21,-10,0,9,0,8,9,3,0,3,6,0,8,-9,\\ &1,-12,-18,0,0,6,0,0,12,3,13,0,0,-3,-9,0,-6,-6,0,3,-3,0,-15,-9,0,4,12,-2,-32,4,\\ &0,-12,0,0,9,-6,-3,0,2,0,1\}. \end{aligned}$$

Problem 16 (Drew Sutherland). Let $\rho_f : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_2(\mathbb{F}_\ell)$ be an odd irreducible mod-ℓ Galois representation associated to a classical modular form f, and let p be a prime not dividing the level of f. Is there a way to determine the conjugacy class of $\rho_f(\mathrm{Frob}_p)$ directly from f (given by its q-expansion, say)?

When the eigenvalues of $\rho_f(\mathrm{Frob}_p)$ are distinct, this is clear, but if $\rho_f(\mathrm{Frob}_p)$ has trace 2 and determinant 1, for example, is it possible to distinguish the conjugacy classes of $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ from the identity without computing separately the torsion of an associated abelian variety?

Problem 17 (John Voight). Is there an efficient (or at least practical) algorithm that, given a genus 2 curve X over $\mathbb{Q}$, computes the isogeny graph of abelian surfaces isogenous to $\mathrm{Jac}(X)$ as principally polarized abelian varieties over $\mathbb{Q}$, and the minimal degree of isogenies between them—like for elliptic curves?

If one allows isogenies that do not respect the principal polarization (so we allow polarizations of arbitrary degree), is the corresponding set finite?