Arithmetic Aspects of Explicit Moduli Problems

Nils Bruin (Simon Fraser University)
Kiran Kedlaya (University of California San Diego)
Samir Siksek (University of Warwick)
John Voight (Dartmouth College)

May 28, 2017–June 2, 2017

1 Overview of the Field

A central theme of modern number theory is understanding *the absolute Galois group of the rational numbers* $G_{\mathbb{Q}} = \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$, and more generally $G_K = \mathrm{Gal}(\overline{K}/K)$ where K is a number field. The principal approach to this has been to study the action of $G_{\mathbb{Q}}$ on objects arising in geometry, especially the p-torsion of elliptic curves. Let E be an elliptic curve defined over $\mathbb{Q}$. This can be given by an equation of the form

$$E \,:\, Y^2 = X^3 + AX + B, \qquad (A, B \in \mathbb{Z}, \quad 4A^3 + 27B^2 \neq 0).$$

The points of E form a group. The action of $G_{\mathbb{Q}}$ on the p-torsion subgroup $E[p]$ gives rise to a mod p representation $\overline{\rho}_{E,p} \;:\; G_{\mathbb{Q}} \to \mathrm{GL}_2(\mathbb{F}_p)$. Such representations are the subject of two of the most important conjectures in number theory. Both are due to Fields Medalist and Abel Prize winner Jean-Pierre Serre: *Serre's uniformity conjecture* (1968) and *Serre's modularity conjecture* (1986). Serre's modularity conjecture was recently proved by Khare and Wintenberger (2009). Another closely related conjecture is the *modularity conjecture for elliptic curves over* $\mathbb{Q}$, proved by Wiles and Taylor (1995) for semistable elliptic curves over $\mathbb{Q}$, and by Breuil, Conrad, Diamond and Taylor (2001) for all elliptic curves over $\mathbb{Q}$. In proving modularity for semistable elliptic curves, Wiles proved Fermat's Last Theorem, a question that had vexed mathematicians for 350 years.

A *modular curve* classifies elliptic curves whose torsion points enjoy certain Galois properties. Understanding the points of modular curves over number fields is key to many great theorems in number theory. Let us mention a few:

(I) Heegner's resolution of Gauss's class number 1 problem required the determination of rational points on various modular curves.

(II) Mazur proved that if E is an elliptic curve defined over $\mathbb{Q}$ and $p > 163$ then E does not have a rational p-isogeny (an equivalent formulation is that $\overline{\rho}_{E,p}$ is irreducible for $p > 163$). The proof involved the determination of rational points on the family of modular curves $X_0(p)$. Mazur's theorem is one of the three great pillars on which the proof of Fermat's Last Theorem rests; the other two are Ribet's level-lowering theorem, and Wiles' modularity of semistable elliptic curves.

(III) Building on earlier work by Mazur and Kamienny, Merel proved the uniform boundedness conjecture: for any $d \geq 1$, there is a B_d such that if E is an elliptic curve over a number field K of degree d and

$p > B_d$ a prime, then E does not have K-rational p-torsion. Merel's theorem involves the study of rational points on symmetric powers of $X_0(p)$ and $X_1(p)$.

(IV) The obstruction to modularity lifting for elliptic curves is represented by rational points on modular curves. The proof of the full modularity theorem for elliptic curves by Breuil, Conrad, Diamond and Taylor required the determination of rational points on several modular curves; this computation was carried out by Elkies.

(IV) Serre's uniformity conjecture that asserts that if $p > 37$ is prime and $E/\mathbb{Q}$ an elliptic curve without complex multiplication then $\overline{\rho}_{E,p}$ is surjective. This conjecture reduces to the determination of rational points on three families of modular curves $X_0(p)$, $X_{\mathrm{s}}^+(p)$, $X_{\mathrm{ns}}^+(p)$.

Beyond modular curves there are equally intriguing but harder moduli problems for curves of higher genus, abelian varieties, abelian varieties with level structure, abelian varieties with certain endomorphism rings, etc.

2 Recent Developments

In recent years there have been many spectacular breakthroughs (both theoretical and algorithmic). These have formed a strong motivation for the workshop. Among them we mention the following:

(I) The proof by Bilu, Parent and Rebolledo [2], [3] of the split Cartan case of Serre's uniformity conjecture: they have determined the rational points on the modular curves $X_{\mathrm{s}}^+(p)$ for $p = 11$ and $p \geq 17$.

(II) The recent proof of modularity of elliptic curves over real quadratic fields by Le Hung, Freitas and Siksek [8]. This required the determination of quadratic points on several complicated modular curves.

(III) Systematic tables of modular curves of small genus due to Zywina and Sutherland.

(IV) Equations for Hilbert modular surfaces for all thirty fundamental discriminants D of level $1 < D < 100$ due to Elkies and Kumar [7].

(V) Work of Derickx, Kamienny, Stein and Stoll [6] who determined the possible prime orders of torsion points on elliptic curves over number fields of degrees 4, 5, 6.

(VI) A database of genus 2 curves due to Booker, Sijsling, Sutherland, Voight and Yasaki [4].

(VII) Work of Bruin and Nasserden [5] elucidating the arithmetic of the Burkhardt quartic which is the moduli space for principally polarized abelian surfaces with full level 3 structure.

3 Open Problems

An open problems session formed one of the highlights of the workshop. The participants were encouraged to suggest good open problems as a means of stimulating further progress in the field.

3.1 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]);
```

3.2 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.

3.3 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

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

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

3.4 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 $X(\mathbb{Q})$.)

3.5 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 Mumford-Tate group is nontrivial ($\text{SL}_2 \times \text{SL}_2 \times \text{SL}_2$) is nonempty and a countable union of components of dimension 1.

- Give an explicit model for one or more components.

- Give explicit points, especially on the Torelli locus.
- 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 $\mathbb{Q}$?)

3.6 Jeroen Sijsling

As in Problem 4, 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.

- The projection onto the first component is degree g. What is the degree of the projection onto the second projection?
- 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?
- What can one say about the sizes of the coefficients in the equations defining Y?

3.7 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
```

3.8 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?

3.9 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 $\mathbb{F}_p(u)$.

3.10 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.)

3.11 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?

3.12 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?

3.13 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.

3.14 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 $\mathbb{Q}$?

3.15 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 an extension of $E_1[2]$ by $E_2[2]$, where E_1 and E_2 are elliptic curves of conductors 11 and 50 respectively. The first few Dirichlet coefficients of the L-function are:

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

3.16 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?

3.17 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?

4 Presentation Highlights

4.1 Balakrishnan and Müller: Rational Points on $X_{\mathrm{ns}}^{+}(13)$

At the workshop Jennifer Balakrishnan and Jan-Steffen Müller created much excitement by announcing the determination of the rational points on the modular curve $X_{\mathrm{ns}}^{+}(13)$, as part of joint work with Netan Dogra, Jan Tuitman and Jan Vonk. This has been a famous open problem for many years. More significantly, it demonstrates the ideas pioneered initially by Minhyong Kim, which were extensively studied at BIRS workshop 07w5063, February 4-9, 2007, have substantial applications to modular curves.

Let $X/\mathbb{Q}$ be a curve of genus $g \geq 2$ with Jacobian J and let ℓ be a prime of good reduction. Using Selmer varieties, Kim defines a decreasing sequence

$$X(\mathbb{Q}_\ell) \supseteq X(\mathbb{Q}_\ell)_1 \supseteq X(\mathbb{Q}_\ell)_2 \supseteq \cdots$$

all containing $X(\mathbb{Q})$. Thanks to the work of Coleman, the 'Chabauty set' $X(\mathbb{Q}_\ell)_1$ is known to be finite provided the 'Chabauty condition' $\operatorname{rank} J(\mathbb{Q}) < g$ holds. In this case one has a practical strategy that often succeeds in computing the set of rational points $X(\mathbb{Q})$. Alas, for the family of modular curves $X_{\mathrm{ns}}^+(p)$ with $p \geq 13$ it is known (assuming BSD) that $\operatorname{rank} J(\mathbb{Q})$ is at least the genus, making the methods of Mazur, Kamienny and Merel (as well as Coleman–Chabauty) inapplicable.

Balakrishnan and Dogra [1] have recently shown that the 'quadratic Chabauty set' $X(\mathbb{Q}_\ell)_2$ is finite provided

$$\operatorname{rank} J(\mathbb{Q}) < g + \operatorname{rank} \mathrm{NS}(J) - 1,$$

where $\mathrm{NS}(J)$ is the Néron-Severi group of $J/\mathbb{Q}$. It is known for modular curves X of genus $g \geq 3$ that $\operatorname{rank} \mathrm{NS}(J) \geq 2$, and thus quadratic Chabauty is strictly more powerful than classical Chabauty in the modular context. The joint work alluded to above turns quadratic Chabauty into a practical computational tool that can be used to attack explicit examples, and the application to $X_{\mathrm{ns}}^+(13)$ is expected to the first of many breakthroughs with this method.

4.2 Zureick-Brown: Mazur's Problem B

Mazur's Problem B (also known as Mazur's vertical uniformity problem) asks for the determination of possible images of the representations $\rho_{E,p^\infty} : G_{\mathbb{Q}} \to \mathrm{GL}_2(\mathbb{Z}_p)$ for elliptic curves E over the rationals and all primes p. For $p > 37$ it is easy to give an answer conditional on Serre's uniformity conjecture. Recently this question has been resolved completely by Rouse and Zureick-Brown [9] for $p = 2$. Zureick-Brown's talk gave a detailed overview of the proof which involves the computation of models of modular curves X_H and rational points on these modular curves for around 700 arithmetically minimal subgroups H of $\mathrm{GL}_2(\mathbb{Z}_2)$.

4.3 Andrew Sutherland: Modular curves of prime-power level with infinitely many rational points

For each open subgroup G of $\mathrm{GL}_2(\hat{\mathbb{Z}})$ containing I and having full determinant there is a a modular curve X_G defined over $\mathbb{Q}$ whose non-cuspidal points parametrize elliptic curves $E/\mathbb{Q}$ such that the image of $\rho_E : G_{\mathbb{Q}} \to \mathrm{GL}_2(\hat{\mathbb{Z}})$ is contained in G. When the index of G is sufficiently large, the curve X_G has genus ≥ 2 and so by Faltings has finitely many rational points. This raise the interesting question of for which G does the modular curve X_G have infinitely many rational points. This talk gave an overview of recent work by Sutherland and Zywina in which they give a full answer to this question where G has prime-power level. They find (up to conjugacy) 248 such groups where $X_G(\mathbb{Q})$ is infinite, with 220 being curves of genus 0, and 28 being elliptic curves with positive rank. This is indeed a step towards Mazur's vertical uniformity conjecture, as for each prime p it gives an explicit classification of possible p-adic images with the possible exception of finitely many j-invariants.

4.4 Pierre Parent: Rational points of Modular Curves–An Arakelovian Point of View

Let p be a prime and let J_e denote Merel's winding quotient of $J_0(p)$; this is the maximal quotient that has analytic rank 0. One knows thanks to deep work of Kolyvagin, Logachev and Kato that $J_e(\mathbb{Q})$ is finite. Write $J \sim J_e \times J_e^\perp$. Let P be a degree d point on $X_0(p)$ (that is a point defined over a number field of degree d). Let $\tilde{P}$ denote the corresponding rational point on the d-th symmetric power $X_0(p)^{(d)}$. The image of this on $J_0(p)$ belongs to the intersection of the two cycles ($J_e^\perp$ + torsion) and $X_0(p)^{(d)}$. Parent's talk explained that knowing the heights and degrees of the two cycles, allows via an arithmetic Bezout theorem, to give an upper bound for the height of the intersection. Of course the smaller the dimension of $J_e^\perp$ (and hence equivalently the larger the dimesion of J_e), the better control we have on the intersection. A theorem of Iwaniec and Sarnak gives

$$\frac{1}{4} + o(p) \leq \frac{\dim(J_e)}{\dim(J_0)} \leq \frac{1}{2} + o(p).$$

A conjecture of Brumer asserts

$$\frac{\dim(J_e)}{\dim(J_0)} = \frac{1}{2} + o(p).$$

Parent sketched a proof of the following theorem: under Brumer's conjecture, the j-height of quadratic points on $X_0(p^2)$ is $O(p^5 \log p)$. Remarkably the bound is independent of the quadratic field!

5 Scientific Progress Made

The workshop schedule was designed to give participants plenty of time for collaboration and discussions. We have asked the participants to report on the progress to existing projects made and also on any new projects initiated during the workshop.

- Samuele Anni and Elisa Lorenzo Garcia: we are designing an algorithm to compute endomorphism rings of threefolds in positive characteristic. Using this algorithm, we are also studying endomorphisms in characteristic zero through liftings, giving a completely algebraic alternative to the known algorithms.

- Samuele Anni and Ekin Özman. We want to study local points on fibred products of X0(p) for different primes p. This is connected to local-global questions studied in Ekin and my thesis from different points of view.

- Samuele Anni and Samir Siksek. A new paper on modularity of elliptic curves over totally real subfields of cyclotomic fields is in preparation.

- Andrew Sutherland, Jeroen Sijsling and John Voight. We have worked on our *Genus 2 automorphy* paper. This is still a work in progress, but we moved the ball forward.

- David Zureick-Brown received lots of advice and help from other participants towards completing Mazur's programme B. The progress made includes:
  - Determination of rational points on several X_H.
  - Andrew Sutherland was able to compute traces of Frobenius at the first 1000 primes for some of the large genus subgroups H. This allowed the recognition that a few pairs of X_H, X_K, with H, K not conjugate, were accidentally isomorphic (and then it was proved). Sutherland will optimize his code to allow computation of zeta functions (and hence, whether J_H is simple, etc) for several of the H for which there are currently no nice equations.

- Maarten Derickx and David Zureick-Brown. We were able to find the rational points on 4 of Maarten's 6 curves, and in one of the remaining 2 cases we were able to rule out most of the standard techniques from working.

- Eric Katz and David Zureick-Brown. We made fair progress on our Buium project (that was the subject of Katz's talk), and some progress on another project (about "Total Jet Spaces").

- Sara Arias-de-Reyna, Elisa Lorenzo Garcia and Christophe Ritzenthaler discussed some aspects of Jacobians of genus 3 curves. This is expected to lead to improvements on the Arias-de-Reyna's work, presented at the workshop, on the realisation of $\mathrm{GSp}_6(\mathbb{F}_\ell)$ as a Galois group of a tamely ramified extension.

- Rachel Pries and Ekin Özman were able to complete their project on p-ranks of trielliptic curves.

- Mark van Hoeij and David Zureick-Brown started an new collaboration. In Zureick-Brown's talk he displayed several curves having high degree plane models. Van Hoeij computed plane models of much lower degrees, which will help Zureick-Brown study the arithmetic of these curves.

- Francesc Fite, Elisa Lorenzo Garcia and Andrew Sutherland. We have continued our work on our paper *Sato-Tate groups of twists of Fermat and Klein quartics*. This is a project we have been working on for a long time, but we finally cracked the last stumbling block during the week and should be able to wrap up the paper shortly.

- Francesc Fite: In my talk I explained the theorem that ensures that if the square of an elliptic curve with CM admits a rational model up to $\overline{\mathbb{Q}}$-isogeny, then the quadratic imaginary field of the CM has either class number 1, class number 2, or class group $C_2 \times C_2$. While one easily shows that all quadratic imaginary fields with class numbers 1 and 2 arise, the question on whether quadratic imaginary fields with class group $C_2 \times C_2$ actually occur was open before the workshop. The afternoon after my talk John Voight showed to me an example having class group $C_2 \times C_2$. We expect to start a collaboration in which we determine exactly which quadratic imaginary fields with class group $C_2 \times C_2$ can arise.

- Nils Bruin, Armand Brumer, Chritophe Ritzenthaler and Jaap Top: we had a discussion which may lead to a new way to compute Serres obstruction for abelian threefolds. We have not proved anything yet but the strategy seems coherent and effective. We consider a non-hyperelliptic genus 4 curve C in $\mathbb{P}^3$ as the intersection of a (unique) quadric Q and cubic over a field K. We ask that the discriminant of Q is a square in K and $Jac(C)$ to have a rational non-zero two-torsion point. We can then construct an unramified double cover $D \to C$ and its Prym is a principally polarized abelian threefold (A, a). We conjecture that if (A, a) is geometrically undecomposable, then (A, a) is the Jacobian of a genus 3 curve over K if and only if the Galois closure of $D \to C \to \mathbb{P}^1$ (the last map coming from any of the rational rulings on Q) is defined over K.

- Christophe Ritzenthaler: I received interesting feedback after my talk from Brumer, Viray, Elkies and Voight. During the problem session, I think we also proved that except for $X(7)$, none of the other $X(n)$ (with $n > 6$) can have a plane model because their automorphism groups are not automorphism groups of plane curves (by results from Harui).

- Ekin Özman and Samir Siksek: we are now many steps closer to completing our project of determining the quadratic points on $X_0(p)$ of genera 3, 4 and 5.

6 Outcome of the Meeting

As the above feedback amply demonstrates, this was a great meeting at which much progress has been made towards fundamental questions in the arithmetic of moduli problems. Many of our participants wrote to tell us how useful the workshop has been to them. We conclude with a few quotes from our participants highlighting the success of the meeting.

Jeroen Sijsling had this to say:

> "The venue and facilities of the workshop were top-notch. The planning encouraged the researchers involved to discuss as much as possible, an invitation that was certainly taken up. Especially useful was the open problems session on Tuesday, where some participants, myself included, asked some open questions of theirs to the audience. My question got resolved quite rapidly by other participants. Also in this way the workshop contributed to advancing its field of research."

Jennifer Johnson-Leung said:

> "The BIRS workshop 17w5065 had a strong positive impact on my research program, I had several valuable interactions with my colleagues. In particular, I learned of certain surfaces that Brumer has recently constructed that he believes to be paramodular. However, he expects the

> representation to have a non-trivial central character. This is not possible in the paramodular theory for essential reasons. He hopes that I and my collaborators will be able to reconcile this. I also had useful conversations with Balakrishnan, Sutherland and Voight about classes of known examples of paramodular surfaces. I found that I had a basic error in my understanding which I was able to correct. I also had the opportunity to meet several colleagues in person for the first time. This makes it much easier for me to write to them with specific questions or ideas. I was able to attend this conference only because of the generous family accommodations. I travel very little due to my husband's disability, and this workshop provided me with the opportunity to interact with collaborators and colleagues very close to my research area. I also learned of useful results and techniques from the lectures."

Andrew Sutherland said:

> "This workshop was an extremely productive one from my perspective. The participants included many leading experts in the field, and I was able to make forward progress on two existing projects with collaborators who were also in attendance, as well as obtaining an entirely new result. I can pinpoint the exact moment when the new insight occurred: it was on the trail up Tunnel Mountain while taking a quick hike I took during the lunch break before the afternoon session. The combination of the theoretical beauty of the mathematical content of the talks and the natural beauty of the environment around BIRS was wonderfully exhilirating."

Finally we quote Armand Brumer, one of our most distinguished participants:

> "It was a great pleasure having a chance to participate in the workshop. Neither the beauty of the surroundings nor the great amenities could make a dent on the stimulating talks and mathematical conversations!"

References

[1] J. S. Balakrishnan and N. Dogra, Quadratic Chabauty and rational points I: p-adic heights, `arXiv:1601.00388`.

[2] Yu. Bilu and P. Parent, Serre's uniformity problem in the split Cartan case, *Annals of Math.* **173** (2011), 569–584.

[3] Yu. Bilu, P. Parent and M. Rebolledo, Rational points on $X_0^+(p^r)(\mathbb{Q})$, *Annales de l'Institut Fourier* **63** (2013), 957–984.

[4] A. R. Booker, J. Sijsling, A. V. Sutherland, J. Voight and D. Yasaki, A database of genus 2 curves over the rational numbers, *LMS Jour. Comp. Math.* **19** (2016), 235–254.

[5] N. Bruin and B. Nasserden, Arithmetic aspects of the Burkhardt quartic threefold, `arXiv:1705.09006`.

[6] M. Derickx, S. Kamienny, W. Stein and M. Stoll, Torsion points on elliptic curves over number fields of small degree, `arXiv:1707.00364`.

[7] N. Elkies and A. Kumar, K3 surfaces and equations for Hilbert modular surfaces, *Algebra & Number Theory* **8** (2014), 2297–2411.

[8] N. Freitas, B. Le Hung and S. Siksek, *Elliptic curves over real quadratic fields are modular*, Inventiones Mathematicae **201** (2015), 159–206.

[9] J. Rouse and D. Zureick-Brown, *Elliptic curves and* 2*-adic images of Galois*, Research in Number Theory (2015), **1**:1.