COLLECTED PROBLEMS FROM THE PROBLEM SESSION

1. Michael Stoll

Setup:
Let C be a sufficiently nice curve, E an elliptic curve and $\pi : C \to E$ a map of degree 2. Then π induces a map $\pi^* : E \to \mathrm{Jac}(C)$. Let Θ be a theta-divisor on $\mathrm{Jac}(C)$.

Question:
Does the following equation for the intersection number hold?

$$\pi^* E \cdot \Theta = 2$$

Remarks:
Michael explicitly checked this equation in the case that $g(C) = 2$ but he is interested in the case of genus 4. One can ask more generally what the intersection number should be when π is a cover of degree n of curves of arbitrary genus?

Results:
It is an exercise in [ACGH85, p. 376, Ex. D-10] to show that for $\pi : C \to H$ a n-sheeted covering over a curve of $g(H) = h$ the corresponding intersection number is given by nh, which answers the more general question.

2. Marta Pieropan

Setup:
Define $S := \{a^2b^3 \mid a, b \in \mathbb{Z},\ \gcd(a, b) = 1,\ \text{and } a, b \text{ square free}\} \subset \mathbb{Z}$.

Question:
Is S thin in $\mathbb{A}^1(\mathbb{Q})$?

Remarks:
The set S lies between the thin set of squares and the not-thin set of squareful numbers (which one gets by removing the conditions on a,b). S is given by those numbers whose p-adic valuations lie all in the set $\{0, 2, 3\}$.

Results:
The following theorem shows that S is *not* a thin set. The proof was given by M. Nakahara.

Theorem 2.1. *The set $S = \{a^2b^3 : a, b \in \mathbb{Z},\ \gcd(a, b) = 1,\ \text{and } a, b \text{ square free}\} \subset \mathbb{A}^1(\mathbb{Q})$ is not thin.*

Proof. By combining Theorems 3.6.1 and 3.6.2 in [Ser08], it follows that for any thin set $T \subset \mathbb{A}^1(\mathbb{Q})$, the reduction map $T \cap \mathbb{A}^1(\mathbb{Z}) \to \mathbb{A}^1(\mathbb{F}_p)$ is not surjective for almost all (all but finitely many) primes p. Hence, it suffices to show that the reduction map $S \to \mathbb{A}^1(\mathbb{F}_p)$ is surjective for infinitely many primes p, but the latter is true in this case for all p.

For $x \in \mathbb{F}_p^\times$ we may choose a lift $a \in \mathbb{Z}$ such that $a \equiv 1/x \bmod p$ and also a lift $b \in \mathbb{Z}$ such that $b \equiv x \bmod p$ and $b \equiv 1 \bmod a$ using the Chinese Remainder Theorem. The square-freeness of a and b is guaranteed by Dirichlet's theorem on arithmetic progressions, i.e. since there are infinitely many primes in an arithmetic progression so one can choose a, b to be distinct primes. Now $a^2b^3 \equiv x \bmod p$ with a, b being distinct primes. □

3. Maarten Derickx

Setup:
Let ε be a character of conductor $p > 2$ and $f \in S_2(p, \varepsilon^2)$ a modular newform of level p and character ε^2.
If $\chi \in \{\varepsilon^{-1}, \varepsilon^{-1*\frac{p+1}{2}}\}$, then $f \otimes \chi \in S_2(\Gamma_0(p^2))$ is a modular form with trivial character.

Question:
Does the following equivalence hold?

$$\chi \text{ is even} \Leftrightarrow \text{analytic rank of } \mathcal{L}(f \otimes \chi, s) \text{ is odd}$$

Remarks:
This question came from the numerical observation that the equivalence holds for all newforms with level up to 300. One can also compute the parity of the analytic rank by looking at the sign of the functional equation.

4. Samir Siksek

Question:
Are there infinitely many elliptic curves $E/\mathbb{Q}$ with $rk(E(\mathbb{Q})) = 2$?

Idea:
One possible way would be to use a family $\mathcal{E}/\mathbb{Q}(T)$ with $rk(\mathcal{E}(\mathbb{Q}(T))) = 2$. The question then is whether one can find infinitely many values $t \in \mathbb{Q}$ s.t. the 2-Selmer rank of $\mathcal{E}_t$ is 2. One can assume that $\#\mathcal{E}(\mathbb{Q}(T))[2] = 4$ so as to make the 2-descent easy.

Remarks:
It is known that there are ∞-many curves $E/\mathbb{Q}$ with $rkE(\mathbb{Q}) \geq 2$.
The question can also be answered positively for $rk(E) \in \{0, 1\}$ for example by considering the family of curves gives by $Y^2 = X(X^2 - p^2)$ for primes p. Here one has:

$$p \equiv 3 \mod 8 \implies rk = 0$$
$$p \equiv 5, 7 \mod 8 \implies rk = 1$$
$$p \equiv 1 \mod 8 \implies rk \in \{0, 2\}$$

Ideas:

- One could try to use families of the form $Y^2 = X(X - f(T))(X - g(T)))$ with $f(T)$, $g(T)$ and $f(T) - g(T)$ "*close to prime*".
- Using the theory developed in the paper [BH16] Bhargava and Ho obtain various bounds on the average ranks of 2,3-Selmer groups of family of elliptic curves with marked points (see [BH]). There might be some interesting/useful ideas/results in these papers.
- In [BH, Theorem 10.1], the authors also show that with density 100% the curves in family F_2 with two marked points (as in the paper) has rank at least 2, but getting an equality seems to be a hard problem (at least by using only the methods in the paper) as the *upper bound* on the average size of the 2-Selmer group in the family F_2 is 12.

5. Tony Várilly-Alvarado

Question:
Does there exist a $K3$-surface $X/\mathbb{Q}$ given by a sextic $w^2 = f_6(x, y, z)$ in the weighted projective space $\mathbb{P}(1, 1, 1, 3)$ with $\mathrm{Pic}(X_{\bar{\mathbb{Q}}}) \cong \mathbb{Z}$ and $\mathrm{Br}(X)[11] \neq 0$?

Remarks:
This question is sort of a spiritual successor to the question of B. Mazur and the elliptic curve case. This is known when the condition of non-trivial 11-torsion in the Brauer group is replaced by non-trivial 2-Torsion and 3-Torsion. The moduli space of K3 surfaces of degree 2 with level structure arising from the Brauer group is provably of general type if level is at least 11, therefore it might not have rational points. Note that if $t \in \mathrm{Br}(X)[11]$ is a non-trivial element, then t represents a transcendental class.

6. Ari Shnidman

Setup:

Let E be an elliptic curve over $\mathbb{F}_q(C)$. Here C is a *nice* curve defined over the finite field $\mathbb{F}_q$ of size $q = p^r$ for some prime power q. This gives a family $\mathcal{E} \to C$ defined over $\mathbb{F}_q$.

Question:

Does there exists a canonical cycle $z \in \mathrm{CH}^2(\mathcal{E} \times_{\mathbb{F}_q} \mathcal{E})$ such that the self intersection number $\langle z, z\rangle \propto \mathcal{L}'(E, 1/2)^2$. Here $\propto$ means up to multiplication by a non-zero constant.

Ideas: We do know some cycles, for example: the diagonal of the graph of Frobenius automorphisms. One idea would be to take a linear combination of all/some of them and see if it works.

7. Samir Siksek

Setup:
Let $B := \{y^n \mid y \in \mathbb{Z},\, n \geq 2\} \subset \mathbb{Z}$ be the set of proper powers and let $S \subset B$ be a finite subset.

Question:
Is there an $f_S \in \mathbb{Z}[X]$ s.t. $f_S(\mathbb{Z}) \cap B = S$?

Remarks:
This question is sort of a reversal of the usual point of view. We often regard equations of the form $y^n = f(x)$ for some $n \geq 2$ and a given $f \in \mathbb{Z}[X]$, i.e. we want to compute $S := f(\mathbb{Z}) \cap B$ for given f. Here we give the set S and look for a matching f.
It might be easier to look at the $B_n := \{y^n \mid y \in \mathbb{Z}\}$ seperately.

Result:
A positive and constructive answer has been given by Stevan Gajovic. Given a finite set $S \subset \mathbb{Z}$ he constructs a polynomial $f_S \in \mathbb{Z}[X]$ s.t. f_S is identity on S and $f_S(\mathbb{Z}\backslash S) \cap B = \emptyset$. The proof of the relevant statement relies on Catalan's conjecture which has been proven in 2002.

Explicitly, define $g(x) := 1 + \prod_{a\in S}(x-a)^4$ and $f(x) := g(x)\,(g(x)(x-1)+1)$. Then f is the identity on S and the two factors of $f(x)$ are coprime for any $x \in \mathbb{Z}$. If $f(x) \in B$, then $g(x) \in B$, i.e. $g(x) - (\prod_{a\in S}(x-a))^4 = 1$ is a solution to Catalan's conjecture.

All of the solutions of $x^a - y^b = 1$ with $a, b > 1$, $x, y \in \mathbb{Z}$ are given by:

(1) $(\pm 3)^2 - 2^3 = 1$
(2) $0^a - (-1)^{2n+1} = 1 \;\; \forall n > 0$
(3) $1^a - 0^b = 1 \;\; \forall a, b > 1$
(4) $(-1)^{2m} - 0^b = 1 \;\; \forall m \geq 1, b > 1$

The exponent 4 in the definition of g implies that $\prod_{a\in S}(x-a) = 0$, i.e. $x \in S$. Hence for $x \in \mathbb{Z}$, $f(x) \in B \iff x \in S$.

8. Maarten Derickx

Inspired by Problem 4:

Question:
Given $n \in \mathbb{N}$, does there exist a family of elliptic curves $\mathcal{E}/\mathbb{Q}(T)$ of rank n, s.t. for all but finitely many $t \in \mathbb{Q}$ we have $rk(\mathcal{E}_t) > n$?

Result:
For $n = 0$, [CS82] look at the family $Y^2 = X(X^2 - (7 + 7T^4)^2)$ over $\mathbb{Q}(T)$. It has rank 0, but for any $t \in \mathbb{Q}$ the corresponding elliptic curve has rank > 1 assuming Selmer's conjecture of elliptic curves.

References

[BH16] Manjul Bhargava and Wei Ho, *Coregular spaces and genus one curves*, Cambridge journal of Mathematics **4** (2016), no. 1, 1-119. ↑2

[BH] Manjul Bhargava and Wei Ho, *On average sizes of Selmer groups and ranks in families of elliptic curves having marked points.* Available at http://www-personal.umich.edu/ weiho/papers/Selmer-averages-families.pdf. ↑2

[ACGH85] E. Arbarello, M. Cornalba, P.A. Griffiths, and J. Harris, *Geometry of Algebraic Curves I*, Vol. 267, Springer Grundlehren, 1985. ↑1

[Ser08] J.P. Serre, *Topics in Galois theory*, 2nd ed., A K Peters Ltd., Wellesley, MA, 2008. ↑1

[CS82] J.W.S. Cassels and A. Schinzel, *Selmer's Conjecture and Families of Elliptic Curves*, Bulletin of the London Mathematical Society **14** (1982), no. 4, 345-348. ↑3