Mathematisches Forschungsinstitut Oberwolfach

Report No. 32/2015

DOI: 10.4171/OWR/2015/32

Explicit Methods in Number Theory

Organised by
Karim Belabas, Talence
Bjorn Poonen, Cambridge MA
Fernando Rodriguez Villegas, Trieste

5 July – 11 July 2015

Abstract. The aim of the series of Oberwolfach meetings on 'Explicit methods in number theory' is to bring together people attacking key problems in number theory via techniques involving concrete or computable descriptions. Here, number theory is interpreted broadly, including algebraic and analytic number theory, Galois theory and inverse Galois problems, arithmetic of curves and higher-dimensional varieties, zeta and L-functions and their special values, and modular forms and functions.

Mathematics Subject Classification (2010): 11xx, 12xx, 13xx, 14xx.

Introduction by the Organisers

The workshop Explicit Methods in Number Theory was organised by Karim Belabas (Talence), Bjorn Poonen (Cambridge MA), and Fernando Rodriguez-Villegas (Trieste), and it took place July 5–11, 2015. Eight previous workshops on the topic had been held, every two years since 1999. The goal of the meeting was to present new methods and results on concrete aspects of number theory. In several cases, this included algorithmic and experimental work, but the emphasis was on the implications for number theory.

There was one 'mini-series' of five expository talks by Andrew Granville and Andrew Sutherland on the breakthrough results on small gaps between primes obtained by Zhang, Maynard and the ensuing two Polymath projects. Some other themes were:

- Arakelov class groups,
- L-functions,

- rational points,
- heuristics and theorems about the proportion of curves satisfying various arithmetic condition.

As always in Oberwolfach, the atmosphere was lively and active, providing an ideal environment for the exchange of ideas and productive discussions. The meeting was well-attended, with 52 participants from a variety of backgrounds, including some young researchers with an OWLG-grant. There were 25 talks of various lengths, and ample time was allotted to informal collaboration.

Acknowledgement: The MFO and the workshop organizers would like to thank the National Science Foundation for supporting the participation of junior researchers in the workshop by the grant DMS-1049268, “US Junior Oberwolfach Fellows”. Moreover, the MFO and the workshop organizers would like to thank the Simons Foundation for supporting Kiran S. Kedlaya and David Roberts in the “Simons Visiting Professors” program at the MFO.

Workshop: Explicit Methods in Number Theory

Table of Contents

Abstracts

Sieve theory and gaps between primes

Andrew Granville and Andrew V. Sutherland

In May of 2013 Yitang Zhang announced the breakthrough result [6] that there are infinitely many pairs of primes separated by a gap of at most 70 million. Zhang's work rests on a modified version of the sieve-theoretic framework laid out by Goldston, Pintz, and Yıldırım [1]. Following Zhang's announcement, a Polymath project [3] was launched with the express objective of sharpening Zhang's result, and within a few months the bound of 70 million was reduced to $4,680$.

Shortly thereafter, James Maynard [2] (and independently, Terence Tao) showed that by modifying the framework of Goldston, Pintz, and Yıldırım in a different way, one that is independent of Zhang's approach, sharper and more general results on prime gaps can be obtained. Maynard's work immediately reduced the bound on prime gaps to 600, and he proved more generally that for every positive integer m, there are infinitely many tuples of $m + 1$ primes that lie within an interval of width at most m^3e^{4m+5}. This led to a second Polymath project that further reduced the bound on prime gaps from 600 to 246, as well as sharpening Maynard's bounds for $m > 1$.

In this series of five expository talks we gave an overview of the remarkable results of Zhang, Maynard, and the two Polymath projects, along with an introduction to the sieve-theoretic methods on which they are based.

References

[1] D.A. Goldston, J. Pintz, and C.Y. Yıldırım, *Primes in tuples I*, Annals of Mathematics **170** (2009), 819–862.

[2] J. Maynard, *Small gaps between primes*, Annals of Mathematics **181** (2015), 383–413.

[3] D.H.J. Polymath, *Bounded gaps between primes*, polymath8 project home page available at `http://michaelnielsen.org/polymath1/index.php?title=Bounded_gaps_between_primes`.

[4] D.H.J. Polymath, *New equidistribution results of Zhang type*, Algebra and Number Theory **8** (2014), 2067–2199.

[5] D.H.J. Polymath, *Variants of the Selberg sieve, and bounded intervals containing many primes*, Research in the Mathematical Sciences **1**.

[6] Y. Zhang, *Bounded gaps between primes*, Annals of Mathematics **179** (2014), 1121–1174.

Some density results in number theory

John Cremona

(joint work with M. Bhargava and T. Fischer)

We discuss a number of results, all of the form "What is the probability that a random equation of the form … has a solution ?" where we will make precise what is meant by *equation* (there will be three families), by *probability* and *random*, and by *solution.* All equations will be (possibly weighted) homogeneous, and we will consider *local solubility* (over $\mathbb{R}$ or $\mathbb{Q}_p$) as well as *global solubility* (over $\mathbb{Q}$) or in some cases *everywhere local solubility* (over all completions of $\mathbb{Q}$).

A. Quadrics in n variables. See `http://arxiv.org/abs/1502.05992`.

We consider quadratic forms $Q(X_1, \dots, X_n)$ in n variables ("n-ary quadrics")

$$Q = \sum_{1 \le i \le j \le n} a_{ij} X_i X_j$$

given by $N = n(n+1)/2$ homogeneous coefficients a_{ij} in a field K, and seek solutions (zeros) in $\mathbb{P}^{n-1}$. We call Q *isotropic over* K if there is a solution in $\mathbb{P}^{n-1}(K)$. We will consider $K = \mathbb{R}$, $K = \mathbb{Q}_p$ (where we may assume $a_{ij} \in \mathbb{Z}_p$ by homogeneity) and $K = \mathbb{Q}$ (with $a_{ij} \in \mathbb{Z}$).

At a prime p: if the coefficients $a_{ij} \in \mathbb{Z}_p$ are chosen at random, what is the probability that Q is isotropic over $\mathbb{Q}_p$? More precisely, what is the p-adic measure $\rho_n(p)$ of the subset

$$\{(a_{ij}) \in \mathbb{Z}_p^N \mid Q \text{ isotropic}/\mathbb{Q}_p\} \subseteq \mathbb{Z}_p^N$$

(or the density of soluble quadrics, since $\mathbb{Z}_p$ has measure 1)?

Over $\mathbb{R}$: let D be a "nice" distribution on $\mathbb{R}^N$, that is, a piecewise smooth rapidly decaying function whose integral over $\mathbb{R}^N$ is 1. What is

$$\rho_n^D(\infty) = \int_{Q \in \mathbb{R}^N \text{ isotropic}/\mathbb{R}} D(Q) \mathrm{d}Q \; ?$$

We consider both the uniform distribution (U) on $[-\frac{1}{2}, \frac{1}{2}]^N$ and the Gaussian Orthogonal Ensemble (GOE). We evaluate $\rho_n^{GOE}(\infty)$ exactly, and have numerical approximations for $\rho_n^U(\infty)$.

To make precise what we mean by taking a random *integral* quadratic form with respect to some distribution D on $\mathbb{R}^N$, and asking for the probability that it is isotropic over $\mathbb{Q}$ or $\mathbb{R}$ or $\mathbb{Q}_p$, we define (for $K = \mathbb{R}$, $\mathbb{Q}$ or $\mathbb{Q}_p$)

$$\rho_n^D(K) = \lim_{X \to \infty} \frac{\sum_{Q \in \mathbb{Z}^N \text{ isotropic}/K} D(Q/X)}{\sum_{Q \in \mathbb{Z}^N} D(Q/X)}.$$

Theorem (A0)**.** $\rho_n^D(\mathbb{R}) = \rho_n^D(\infty)$*, and* $\rho_n^D(\mathbb{Q}_p) = \rho_n(p)$ *(independent of* D*).*

Theorem (A1)**.** $\rho_n^D(\mathbb{Q}) = \rho_n^D(\infty) \prod_p \rho_n(p) = \rho_n^D(\mathbb{R}) \prod_p \rho_n^D(\mathbb{Q}_p)$.

Theorem (A2)**.** *The probability* $\rho_n(p)$ *that a random* n*-ary quadric over* $\mathbb{Z}_p$ *is isotropic over* $\mathbb{Q}_p$ *is*

n	$\rho_n(p)$
1	0
2	1/2
3	$1 - \frac{p}{2(p+1)^2}$
4	$1 - \frac{p^3}{4(p+1)^2(p^4+p^3+p^2+p+1)}$
≥ 5	1

The proof is uniform in p and n, and gives a new proof that all quadrics in ≥ 5 variables are isotropic over $\mathbb{Q}_p$, and an algorithm for deciding isotropy for $n \leq 4$.

Theorem (A3, joint also with J. Keating and N. Jones (Bristol))**.** *The probability that a GOE-random n-ary quadric over $\mathbb{R}$ is isotropic is*

$$\rho_n^{GOE}(\infty) = 1 - \frac{\mathrm{Pf}(S)}{2^{(n-1)(n+4)/4}\prod_{m=1}^{n}\Gamma(m/2)},$$

where S is the skew-symmetric matrix of size $2\lceil n/2 \rceil$ whose i, j entry is

$$\begin{cases} 2^{i+j-2}\Gamma\left(\frac{i+j}{2}\right)\left(\beta_{\frac{1}{2}}(\frac{i}{2},\frac{j}{2}) - \beta_{\frac{1}{2}}(\frac{j}{2},\frac{i}{2})\right) & \textit{for } i < j \leq n; \\ 2^{i-1}\Gamma\left(\frac{i}{2}\right) & \textit{for } i < j = n+1 \ (n \textit{ odd}). \end{cases}$$

n	$\rho_n^{GOE}(\infty)$	
1	0	0
2	$\frac{1}{2}\sqrt{2}$	0.7071067811
3	$\frac{1}{2} + \sqrt{2}\pi^{-1}$	0.9501581580
4	$\frac{1}{2} + \frac{1}{8}\sqrt{2} + \pi^{-1}$	0.9950865814
5	$\frac{3}{4} + (\frac{2}{3} + \frac{1}{12}\sqrt{2})\pi^{-1}$	0.9997197706
6	$\frac{3}{4} + \frac{7}{64}\sqrt{2} + (\frac{37}{48} - \frac{1}{3}\sqrt{2})\pi^{-1}$	0.9999907596
7	$\frac{7}{8} + (\frac{47}{120} + \frac{109}{480}\sqrt{2})\pi^{-1} - \frac{32}{45}\sqrt{2}\pi^{-2}$	0.9999998239
...	...	...
n	$\in \mathbb{Q}(\sqrt{2})[\pi^{-1}]$	≈ 1

Corollary. *If D=U or GOE then*

$$\rho_n^D(\mathbb{Q}) = \begin{cases} 0 & \textit{if } n \leq 3; \\ \rho_4^D(\infty)\prod_p\left(1 - \frac{p^3(p-1)}{4(p+1)^2(p^5-1)}\right) & \textit{if } n = 4; \\ \rho_n^D(\infty) & \textit{if } n \geq 5. \end{cases}$$

In particular,

$$\rho_4^{GOE}(\mathbb{Q}) = \left(\frac{1}{2} + \frac{1}{8}\sqrt{2} + \frac{1}{\pi}\right)\prod_p\left(1 - \frac{p^3(p-1)}{4(p+1)^2(p^5-1)}\right)$$
$$\approx 0.983,$$

$\rho_n^{GOE}(\mathbb{Q}) = \rho_n^{GOE}(\infty) > 0.999$ *for* $n \geq 5$, *and* $\rho_n^{GOE}(\mathbb{Q}) = 0$ *for* $n \leq 3$.

(B) Ternary cubics. See `http://arxiv.org/abs/1311.5578`.

We consider ternary cubic forms $f(X, Y, Z)$ with 10 coefficients in K, and seek solutions (zeros) in $\mathbb{P}^2(K)$. Again, by homogeneity, when $K = \mathbb{Q}$ or $K = \mathbb{Q}_p$ we may assume that the coefficients are integral. Since there is no Hasse principle for plane cubics, over $\mathbb{Q}$ we will only ask for everywhere local solubility. As solubility over $\mathbb{R}$ is obviously automatic, this amounts to solubility over $\mathbb{Q}_p$ for all primes p.

Define $\rho(p)$ to be the probability that a random (with respect to the p-adic measure on $\mathbb{Z}_p^{10}$) ternary cubic form over $\mathbb{Z}_p$ has a $\mathbb{Q}_p$-rational point. We furthermore define $\rho(\mathbb{Q})$ to be the probability that a random integral ternary cubic has

$\mathbb{Q}_p$-rational points for all p (we do not consider global solubility). Real solubility is now automatic, and we do not need to specify a distribution on the space $\mathbb{R}^{10}$.

As with quadrics, we find that the the probability of a random integral ternary cubic (with respect to any nice distribution) has a $\mathbb{Q}_p$-point is the same as $\rho(p)$, the probability that a random cubic over $\mathbb{Z}_p$ has a $\mathbb{Q}_p$-point.

Theorem (B1)**.** $\rho(\mathbb{Q}) = \prod_p \rho(p)$.

Theorem (B2)**.** *For all primes p, the probability that a random plane cubic over $\mathbb{Q}_p$ has a $\mathbb{Q}_p$-rational point is*

$$\rho(p) = 1 - f(p)/g(p),$$

where

$$\begin{aligned} f(p) &= p^9 - p^8 + p^6 - p^4 + p^3 + p^2 - 2p + 1, \\ g(p) &= 3(p^2+1)(p^4+1)(p^6+p^3+1). \end{aligned}$$

Note that $f(p)/g(p) \sim 1/3p^3$, so $\rho(p) \to 1$ rapidly as $p \to \infty$: $\rho(2) = 0.98319$, $\rho(3) = 0.99259$, $\rho(5) = 0.99799$, $\rho(7) = 0.99918$.

Corollary (B3)**.** *A random integral plane cubic is everywhere locally soluble with probability $\rho(\mathbb{Q}) = \prod_p (1 - f(p)/g(p)) \approx 0.97256$.*

This Corollary is used in Manjul Bhargava's result that a positive proportion of plane cubics fail the Hasse principle.

(C) Elliptic quartics. We consider quartic (hyper)elliptic equations $Z^2 = f(X,Y)$ with f a binary form of degree 4 over K, defined by 5 coefficients. Again, over $\mathbb{Q}$ we only ask for everywhere local solubility; solubility over $\mathbb{R}$ is no longer trivial.

Define $\rho(p)$ to be the probability that a random (with respect to the p-adic measure on $\mathbb{Z}_p^5$) binary quartic form $f(X,Y)$ over $\mathbb{Z}_p$ is soluble, in the sense that the curve $Z^2 = f(X,Y)$ has a $\mathbb{Q}_p$-rational point in $\mathbb{P}_{1,1,2}$. We give a formula for $\rho(p)$ all *odd* primes p, which needs adjustment at $p = 2$. However, if we instead consider *generalized binary quartics*, equations of the form $Z^2 + g(X,Y)Z = f(X,Y)$ with $\deg(g) = 2$ and $\deg(f) = 4$, distributed over $\mathbb{Z}_p^8$, then we obtain a uniform formula for all p (which agrees with the non-generalized formula for odd p).

Define $\rho(\mathbb{Q})$ to be the probability that a random integral binary quartic quartic has $\mathbb{Q}_p$-rational points for all p and real points; here we do need to specify a distribution D on $\mathbb{R}^5$. Again we do not consider global solubility.

Theorem (C1)**.** $\rho(2) = \frac{23087}{24529}$*, and for* $p \geq 3$*:*

$$\rho(p) = \frac{F(p)}{G(p)} = \frac{8p^{10} + 8p^9 - 4p^8 + 2p^6 + p^5 - 2p^4 + p^3 - p^2 - 8p - 5}{8(p+1)(p^9-1)}.$$

The density in $\mathbb{Z}_p^8$ of pairs of forms $f, g \in \mathbb{Z}_p[X,Y]$ of degree 4 and 2 for which the curve $Z^2 + g(X,Y)Z = f(X,Y)$ has a $\mathbb{Q}_p$-rational point is $\rho(p)$ (as above) for $p \geq 3$ and for $p = 2$ is $F(2)/G(2) = 11887/12264$.

The probability $\rho(\mathbb{R})$ that a random real quartic f is not negative definite is between 0.872 and 0.875 for the uniform distribution; the exact value is not known.

Theorem (C2)**.** *When genus* 1 *curves of the form* $Z^2 = f(X,Y)$*, with* $f \in \mathbb{Z}[X,Y]$ *homogeneous quartic, are ordered by the height of* f*, the proportion which are everywhere locally soluble is*

$$\rho(\mathbb{Q}) = \rho(\mathbb{R}) \cdot \frac{23087}{24529} \cdot \prod_{p\geq 3} \frac{F(p)}{G(p)} \approx 0.759.$$

In future we will treat similar questions for hyperelliptic curves of higher genus.

Sums of seven cubes

Samir Siksek

1. Brief History and Main Theorem

A long-standing conjecture states that every positive integer other than

$$15,\ 22,\ 23,\ 50,\ 114,\ 167,\ 175,\ 186,\ 212,$$
$$231,\ 238,\ 239,\ 303,\ 364,\ 420,\ 428,\ 454$$

is a sum of seven (non-negative) cubes. This was first observed by Jacobi in 1851 on the basis of extensive calculations performed by the famous computationalist Zacharias Dase.

In 1943 Linnik [6] showed that every sufficiently large integer is the sum of seven cubes. A substantially simpler proof (though still ineffective) was given by Watson [9]. Linnik's seven cubes theorem was first made effective by McCurley [7], who showed that it is true for integers $> \exp(\exp(13.94))$. Ramaré [8] improved this to $\exp(524) \approx 3.72 \times 10^{227}$. This bound is way beyond computer searches. In [3], it is shown that every integer between $1\,290\,741$ and 10^{16} is a sum of five cubes. As observed in [8], combining this with the greedy algorithm [1, Lemma 3], we can easily deduce that every integer $455 \leq N \leq \exp(78.7) \approx 1.51 \times 10^{34}$ is the sum of seven cubes.

There has been a number of partial results concerning sums of seven cubes. Bertault, Ramaré and Zimmermann [1] show that every non-negative integer which is a cubic residue modulo 9 and an invertible cubic residue modulo 37 is a sum of 7 cubes. Bolkan and Elkies [2] show that every multiple of 4 greater than 454 is the sum of seven cubes, whilst Elkies [4] shows the same for integers $\equiv 2 \pmod 4$.

The main theorem proved in this talk is the following.

Theorem. *Every positive integer other than*

$$15,\ 22,\ 23,\ 50,\ 114,\ 167,\ 175,\ 186,\ 212,\ 231,\ 238,\ 239,\ 303,\ 364,\ 420,\ 428,\ 454$$

is the sum of seven cubes.

2. The Main Criterion

Let $\mathscr{K} = \exp(524)$ and $\mathscr{K}' = \exp(78.7)$. By the results of [8] and of [3], it is sufficient to prove that every integer $\mathscr{K}' \le N \le \mathscr{K}$ is the sum of seven cubes. The results of [2] and [4] allow us to restrict ourselves to odd integers N (our method can certainly be adapted to deal with even integers, but restricting ourselves to odd integers brings coherence to our exposition). We provide a criterion in the succeeding Proposition for all odd integers N in a range $K_1 \le N \le K_2$ to be sums of seven cubes. The remainder of the proof involves subdividing the interval $[\mathscr{K}', \mathscr{K}]$ into around 5000 subintervals and verifying the criterion by a computer computation that took roughly 14 days.

Let x be a real number and m be a positive integer. Define the **quotient** and **remainder** obtained on dividing x by m as

$$Q(x,m) = \lfloor x/m \rfloor, \qquad R(x,m) = x - Q(x,m) \cdot m.$$

In particular, $R(x,m)$ belongs to the half-open interval $[0,m)$. If $x \in \mathbb{Z}$ then $R(x,m)$ is the usual remainder on dividing by m, and $x \equiv R(x,m) \pmod{m}$. Let M be a positive integer such that $m \mid M$. Let ε and δ be real numbers satisfying $0 \le \varepsilon < \delta \le 1$. Define

$$\mathfrak{J}(M,m,\varepsilon,\delta) = \Big\{ x \in [0,M) \ : \ R(x,m) \in [0,m) \setminus [\varepsilon \cdot m, \delta \cdot m) \Big\} \tag{1}$$

$$= \bigcup_{k=0}^{(M/m)-1} km + ([0,m) \setminus [\varepsilon \cdot m, \delta \cdot m)). \tag{2}$$

Given a set of positive integers $\mathcal{W}$, and sequences $\underset{\sim}{\varepsilon} = (\varepsilon_m)_{m \in \mathcal{W}}$, $\underset{\sim}{\delta} = (\delta_m)_{m \in \mathcal{W}}$ of real numbers satisfying $0 \le \varepsilon_m < \delta_m \le 1$ for all $m \in \mathcal{W}$, we define

$$\mathfrak{J}(\mathcal{W}, \underset{\sim}{\varepsilon}, \underset{\sim}{\delta}) = \bigcap_{m \in \mathcal{W}} \mathfrak{J}(M, m, \varepsilon_m, \delta_m) \tag{3}$$

where $M = \operatorname{lcm}(\mathcal{W})$.

Proposition. *Let $0 < K_1 < K_2$ be real numbers. Let $\mathcal{W}$ be a non-empty finite set of integers such that every element $m \in \mathcal{W}$ satisfies*

(i) m is a squarefree positive integer,
(ii) $3 \mid m$,
(iii) every prime divisor of $m/3$ is $\equiv 5 \pmod 6$.

Suppose moreover, that for each $m \in \mathcal{W}$, there are real numbers ε_m, δ_m satisfying

(iv) $0 \le \varepsilon_m < \delta_m \le 1$,
(v) $K_1 \ge (8\delta_m^3 + 1/36)m^3 + 3m/4$,
(vi) $K_2 \le (8\varepsilon_m^3 + 1/18)m^3 + m/2$.

Write $M = \operatorname{lcm}(\mathcal{W})$. Let $\mathfrak{S} \subset [0,1]$ be a finite set of rational numbers a/q (here $\gcd(a,q) = 1$) with denominators q bounded by $\sqrt[3]{M/2K_2}$. Suppose that

$$\mathfrak{J}(\mathcal{W},\underset{\sim}{\varepsilon},\underset{\sim}{\delta}) \subseteq \bigcup_{a/q\in\mathfrak{S}} \left(\frac{a}{q}M - \frac{\sqrt[3]{M/16}}{q}\ ,\ \frac{a}{q}M + \frac{\sqrt[3]{M/16}}{q}\right). \tag{4}$$

Then every odd integer $K_1 \leq N \leq K_2$ *is the sum of seven non-negative cubes.*

References

[1] F. Bertault, O. Ramaré, and P. Zimmermann, *On sums of seven cubes*, Math. Comp. **68** (1999), 1303–1310.

[2] K. O. Boklan and N. D. Elkies, *Every multiple of* 4 *except* 212*,* 364*,* 420*, and* 428 *is the sum of seven cubes*, (2009), Preprint, `arXiv:0903.4503`.

[3] J.-M. Deshouillers, F. Hennecart, and B. Landreau, 7 373 170 279 850, Math. Comp. **69** (2000), 421–439.

[4] N. D. Elkies, *Every even number greater than* 454 *is the sum of seven cubes*, (2009), Preprint, `arXiv:1009.3983`.

[5] C. G. J. Jacobi, *Über die zusammensetzung der zahlen aus ganzen positiven cuben; nebst einer tabelle für die kleinste cubenanzahl, aus welcher jede zahl bis* 12000 *zusammengesetzt werden kann*, Journal für die reine und angewandte Mathematik **XLII** (1851).

[6] Yu. V. Linnik, *On the representation of large numbers as sums of seven cubes*, Rec. Math. [Mat. Sbornik] N. S. **12** (1943), 218–224.

[7] K. S. McCurley, *An effective seven cube theorem*, J. Number Theory **19** (1984), 176–183.

[8] O. Ramaré, *An explicit result of the sum of seven cubes*, Manuscripta Math. **124** (2007), 59–75.

[9] G. L. Watson, *A proof of the seven cube theorem*, J. London Math. Soc.**26** (1951), 153–156.

Explicit Chern class maps and hyperbolic 3-manifolds

Frank Calegari

(joint work with S. Garoufalidis and D. Zagier)

Zagier and Garoufalidis first computed a (conjectural) invariant by investigating generalizations of the Volume Conjecture. For a certain class of finite volume 3-manifolds M, they defined a (conjectural) invariant for each prime number p with the following properties:

(1) The invariant appears to lie in $F(\zeta)^{\times}/F(\zeta)^{\times p}$, where ζ is a pth root of unity and F is the invariant trace field of M.

(2) In many circumstances, the invariant was actually a unit — that is, it was an element of $\mathcal{O}^{\times}_{F(\zeta)}$.

In 2011, Zagier asked the speaker whether there was a direct construction of such an invariant. A finite volume hyperbolic three manifold typically gives rise to an element of the Bloch group $B(F)$, which, (up to torsion dividing μ_F) is isomorphic to $K_3(F)$. Because of this, the natural suggestion was to start with the Chern class map of Soulé, which gives rise to a map:

$$K_3(F) \to H^1(F, \mathbb{Z}_p(2)).$$

Given such a map, one can compose it with the following maps:

$$H^1(F,\mathbb{Z}_p(2)) \to H^1(F,\mathbb{Z}/p\mathbb{Z}(2)) \to H^1(F(\zeta),\mathbb{Z}/p\mathbb{Z}(2))^G,$$

given by reduction modulo the prime p followed by restriction, where

$$G = \mathrm{Gal}(F(\zeta)/F) \subset (\mathbb{Z}/p\mathbb{Z})^\times.$$

Because $\mathbb{Z}/p\mathbb{Z}(2) = \mu_p$ as a module over the absolute Galois group of $F(\zeta_p)$, one has further isomorphisms:

$$H^1(F(\zeta), \mathbb{Z}/p\mathbb{Z}(2))^G = H^1(F(\zeta), \mu_p)^{G=\chi^{-1}} = \left(F(\zeta)^\times / F(\zeta)^{\times p}\right)^{G=\chi^{-1}},$$

where χ^{-1} corresponds to the action of G on $\mathbb{Z}/p\mathbb{Z}(-1)$, and the second isomorphism comes from Hilbert's Theorem 90. One naturally conjectures that the invariant of Zagier and Garoufalidis is equal to this Chern class. In this talk, the main problem we address is as follows:

> *The Bloch group $B(F)$ has a very explicit presentation; can one give a formula for the Chern class map directly on $B(F)$?*

It turns out that there is a nice such formula, which comes down to properties of the following "function." Let $X \in F$, and let $x^p = X$ where $x \in H$ and H is the maximal extension of $F(\zeta_p)$ obtained by taking pth roots of every element of F. Then let

$$D(X) = \prod_{k=0}^{p-1} (1 - \zeta^k x)^k \in H^\times / H^{\times p}.$$

The main result is as follows. Let $[c] = \sum a_i [X_i]$ be an element of the Bloch group $B(F)$. Assume that p does not divide $w_F = |\mu_F|$. Then the quantity

$$D([c]) := \prod D(X_i)^{a_i} \in H^\times / H^{\times p}$$

descends to an element in the image of $F(\zeta_p)^\times / F(\zeta_p)^{\times p}$ under the restriction map:

$$\left(F(\zeta_p)^\times / F(\zeta_p)^{\times p}\right) \to H^\times / H^{\times p}.$$

Moreover, this descended class depends only on $[c]$ as an element of $B(F)$, and moreover the descended class can be chosen (uniquely) so as to lie in the χ^{-1}-invariant part under the action of G. Finally, this map coincides with the map above constructed from the Chern class map, at least up to a universal constant.

Congruences and formal groups

Masha Vlasenko

Congruences for the coefficients of the logarithm of a formal group law

A commutative (1-dimensional) formal group law over a commutative ring R is a formal power series $F(X, Y) \in R[[X, Y]]$ satisfying

$$\begin{aligned} F(X,0) &= F(0,X) = X \\ F(F(X,Y),Z) &= F(X,F(Y,Z)) \text{ (associativity)} \\ F(X,Y) &= F(Y,X) \text{ (commutativity).} \end{aligned}$$

If R is a characteristic zero ring (i.e. $R \to R \otimes \mathbb{Q}$ is injective), then there exists a unique formal power series $f(X) = X + \ldots \in R \otimes \mathbb{Q}$ such that

$$F(X,Y) = f^{-1}(f(X) + f(Y)) .$$

This power series f is called the logarithm of F and denoted $f = \log_F$. One can show that the coefficients of the logarithm $\log_F(X) = \sum_{n=1}^{\infty} a_n X^n$ satisfy $na_n \in R$.

Conversely, every power series $f = X + \ldots \in R \otimes \mathbb{Q}[[X]]$ gives a commutative formal group law $F(X,Y) = f^{-1}(f(X) + f(Y))$ over $R \otimes \mathbb{Q}$. Our result below characterizes f for which we actually obtain $F \in R[[X,Y]]$. Let's fix a prime number p. We assume that the ring R is endowed with a Frobenius endomorphism $\Phi \in \mathrm{End}(R)$, that is we have $\Phi(r) \equiv r^p \mod pR$ for every $r \in R$. Consider the sequence $\{b_n = (n+1)a_{n+1}, n \geq 0\}$. For given p, there exists a unique sequence $\{c_n, n \geq 0\}$ satisfying

$$b_n \;=\; \sum_{n = n_1 * \ldots * n_r} c_{n_1} \cdot \Phi^{\ell(n_1)}(c_{n_2}) \ldots \Phi^{\ell(n_1)+\ldots+\ell(n_{r-1})}(c_{n_r}) ,$$

where the sum runs over all decompositions of the expansion of n to the base p into parts (and the number of parts r varies from 1 to the length of the expansion of n to the base p respectively).

Theorem 1 (M.V., Eric Delaygue, 2015). *$F \in R \otimes \mathbb{Z}_{(p)}[[X,Y]]$ if and only if*

$$c_{mp^k - 1} \in p^k R \quad \text{for all} \quad m > 1, k \geq 0 .$$

An application: p-adic analytic formulas for Eisenstein polynomials

From now on we assume that $R = \mathbb{Z}$ and Φ is the identity morphism for every p. Let $F(X,Y) \in \mathbb{Z}[[X,Y]]$ be a formal group law and $f(X) = \log_F(X) \in \mathbb{Q}[[X]]$ be its logarithm. For every prime p there is a polynomial $P_p(T) \in \mathbb{Z}_p[T]$ called the *Eisenstein polynomial* of F. Here is a method to construct the Eisenstein polynomial due to Taira Honda. We have $\mathbb{Z} \subset \mathbb{Z}_{(p)} \subset \mathbb{Z}_p$. Consider F as a group law over $\mathbb{Z}_{(p)}$. Every formal group law over a $\mathbb{Z}_{(p)}$-algebra is of 'functional equation type'. In our case it means that the logarithm $f(X)$ satisfies

$$f(X) \;-\; \frac{1}{p} \sum_{s=1}^{\infty} v_s f(X^{p^s}) \in \mathbb{Z}_{(p)}[[X]]$$

for some sequence of numbers $v_s \in \mathbb{Z}_{(p)}$. Formal groups over $\mathbb{Z}_p$ are classified by their Eisenstein polynomials. Let

$$h = \inf\{ s \geq 1 \;:\; v_s \in \mathbb{Z}_{(p)}^{\times} \} .$$

If $h < \infty$, then there is a unique unit $\theta(T) \in \mathbb{Z}_p[[T]]^{\times}$ such that

$$\Big(p \;-\; \sum_{s=1}^{\infty} v_s T^s \Big) \theta(T) \;=\; p + \sum_{i=1}^{h} \alpha_i T^i$$

where $\alpha_h \in \mathbb{Z}_p^\times$ and $\alpha_i \in p\mathbb{Z}_p$ for $1 \leq i < h$. The right-hand side here is the Eisenstein polynomial $P_p(T)$. $h = \deg P_p(T)$ is called *the height* of $F(X,Y)$ at p. Two group laws are isomorphic over $\mathbb{Z}_p$ if and only if their Eisenstein polynomials coincide. (If $h = \infty$, the group law is isomorphic to the additive group law $G(X,Y) = X + Y$.)

Example $\hat{\mathbb{G}}_m$. For every odd prime p the Eisenstein polynomial of the group law $F(X,Y) = X + Y + XY$ is given by $P_p(T) = p - T$. Indeed, the logarithm of this group law is given by $f(X) = \log(1+X) = \sum_{n=1}^\infty \frac{(-1)^{n-1}}{n} X^n$, which satisfies $f(X) - \frac{1}{p} f(X^p) \in \mathbb{Z}_{(p)}[[X]]$. Therefore $h = 1$, $\theta(T) = 1$ and $P_p(T) = p - T$.

Congruences from Theorem 1 allow us to give p-adic analytic formulas for the Eisenstein polynomial. This work is in progress. Let's write $\log_F(X) = f(X) = \sum_{n=1}^\infty \frac{a_n}{n} X^n$ with $a_n = b_{n-1} \in \mathbb{Z}$. We will state the result for the case of height 1. ($h = 1 \Leftrightarrow p \not| a_p$. We have $a_{p^s} \equiv a_p^s \mod p$, so $p \not| a_{p^s}$ for all s in this case.)

Theorem 2. *Suppose $p \not| a_p$. Then there exists a unique unit $\alpha \in \mathbb{Z}_p^\times$ such that*

$$a_{p^s} \equiv \alpha \, a_{p^{s-1}} \mod p^s$$

for every $s \geq 1$. The Eisenstein polynomial is given by $P_p(T) = p - \alpha T$.

For example, the respective formal group law is isomorphic to $\hat{\mathbb{G}}_m$ over $\mathbb{Z}_p$ if and only if $\alpha = 1$ or, equivalently, one has $a_{p^s} \equiv a_{p^{s-1}} \mod p^s$ for all $s \geq 1$. In [2] Beukers showed this congruence for the Apéry sequences

$$b_n = \sum_{k=0}^n \binom{n}{k}^2 \binom{n+k}{k} \quad \text{and} \quad b_n = \sum_{k=0}^n \binom{n}{k}^2 \binom{n+k}{k}^2$$

for all $p > 3$. (In terms of $b_n = a_{n+1}$ it reads as $b_{p^s-1} \equiv b_{p^{s-1}-1} \mod p^s$ for all $s \geq 1$.) He also pointed out that the respective formal groups are isomorphic to $\hat{\mathbb{G}}_m$ over $\mathbb{Z}[\frac{1}{2}, \frac{1}{3}]$.

Formal groups arising from the middle cohomology of hypersurfaces

Let $\Lambda(x_1, \ldots, x_N) \in R[x_1^{\pm 1}, \ldots, x_N^{\pm 1}]$ be a Laurent polynomial and $\Delta \subset \mathbb{R}^N$ be the Newton polytope of Λ. We consider the set $J = \Delta^\circ \cap \mathbb{Z}^N$ of internal integral points of Δ. Let $h = \#J$. Consider the sequence of $h \times h$ matrices with entries in R given by

$$(\beta_n)_{u,v \in J} = \text{the coefficient of } x^{(n+1)v-u} \text{ in } \Lambda(x)^n .$$

Theorem 3. *The tuple of h power series $\{f_u(X); u \in J\}$ in h variables $X = \{x_v; v \in J\}$ given by*

$$f(X) = \sum_{n=1}^\infty \frac{\beta_{n-1}}{n} X^n$$

is the logarithm of an h-dimensional formal group law over R.

To prove this theorem we show explicit congruences like in Theorem 1, and apply Hazewinkel's functional equation lemma. It seems that these formal group laws appeared in [3] for the first time. Under certain assumptions (Λ comes from a homogeneous polynomial of degree $d > N$, R is flat over $\mathbb{Z}$). Jan Stienstra showed that the Artin–Mazur functor $H^{N-1}(X, \widehat{\mathbb{G}_{m,X}})$ for the projective hypersurface X given by $\Lambda(x) = 0$ is a formal group isomorphic to the one from Theorem 3.

Assume for simplicity that $R = \mathbb{Z}$. We also have a result similar to Theorem 2.

Theorem 4. (i) *We have* $\beta_{p^s-1} \equiv \beta_{p-1}^s \mod p$ *for all* $s \geq 1$.

(ii) *Assume that* $p \nmid \det \beta_{p-1}$. *Then all matrices* β_{p^s-1} *are invertible over* $\mathbb{Z}_{(p)}$ *and there exists a unique invertible* $h \times h$ *matrix* α *with entries in* $\mathbb{Z}_p$ *such that*

$$\alpha \equiv \beta_{p^s-1}\beta_{p^{s-1}-1}^{-1} \mod p^s .$$

(iii) *Let* $X_p = X \times_{Spec\,\mathbb{Z}} Spec\,\mathbb{F}_p$ *be the fibre of* X *at* p. *Assume that there exists a smooth projective variety* Y *over* $\mathbb{F}_p$ *and a morphism* $\pi : Y \to X_p$ *such that* $\pi_*\mathcal{O}_Y = \mathcal{O}_{X_p}$ *and* $R^i\pi_*\mathcal{O}_Y = 0$ *for* $i \geq 1$. *Let*

$$P_p(T) = \det(1 - T\,Frob_p | H^{N-1}_{crys}(Y)) \in \mathbb{Z}[T]$$

be the characteristic polynomial of the Frobenius operator acting on the middle crystalline cohomology of Y. *Then*

$$P_p(\alpha) = 0\,,$$

where α *is the invertible* $h \times h$ *matrix over* $\mathbb{Z}_p$ *from (ii). In particular, the characteristic polynomial of* α *divides* $P_p(T)$.

Parts (i) and (ii) are proved in [5]. The last part is a combination of (ii) with Stienstra's congruences from [4]. Namely, let's write

$$P_p(T) = 1 + \alpha_1 T + \alpha_2 T^2 + \ldots \alpha_m T^m$$

where $m = \dim H^{N-1}(X)$. Stienstra showed that under the assumptions in (iii) we have

$$\beta_{n-1} + \alpha_1\beta_{n/p-1} + \ldots + \alpha_m\beta_{n/p^m-1} \equiv 0 \mod p^{\mathrm{ord}_p(n)}$$

for all n, where we agree that $\beta_n = 0$ whenever $n \notin \mathbb{N}$. These congruences generalize congruences of Atkin and Swinnerton-Dyer for elliptic curves.

For example, the sequence $b_n = \sum_{k=0}^{n} \binom{n}{k}^2 \binom{n+k}{k}$ is the sequence of constant terms of the Laurent polynomial $\Lambda(x,y) = (1+x)(1+y)(1+x+y)/x/y$. The variety of its zeroes consists of three lines and the respective formal group is isomorphic to $\widehat{\mathbb{G}}_m$ as we mentioned earlier. Let's deform this polynomial a bit to get

$$\Lambda'(x,y) = \frac{(1+x)(1+y)(1+x+y)}{xy} - 1\,.$$

The projectivization of the variety $\Lambda'(x,y) = 0$ is the elliptic curve E of conductor 11. (I used Magma to compute the conductor). Let $\{b_n; n \geq 0\}$ be the sequence of constant terms of Λ'. By (iii) for every $p \neq 11$ the number $\beta = \lim_{s\to\infty} b_{p^s-1}/b_{p^{s-1}-1}$ is the p-adic unit solution of the equation $T^2-a_pT+p=0$, where $a_p = p+1-\#E(\mathbb{F}_p)$ is the Frobenius trace for this elliptic curve.

p	a_p	β
3	-1	$2+3^2+2\cdot 3^3+2\cdot 3^4+O(3^5)$
5	1	$1+4\cdot 5+3\cdot 5^2+O(5^3)$
7	-2	$5+3\cdot 7+4\cdot 7^2+O(7^3)$
13	4	$4+3\cdot 13+O(13^2)$

References

[1] M. Hazewinkel, *Formal groups and applications*, Academic Press, New York (1978).

[2] F. Beukers, *Some congruences for Apery numbers*, Journal of Number Theory **21** (1985), 141–155.

[3] J. Stienstra, *Formal group laws arising from algebraic varieties*, American Journal of Mathematics **109** (1987), 907–925.

[4] J. Stienstra, *Formal groups and congruences for L-functions*, American Journal of Mathematics **109** (1987), 1111–1127.

[5] M. Vlasenko, *Explicit p-adic unit-root formulas for hypersurfaces*, Preprint, arXiv:1501.04280.

Computing Elliptic Curves over Number Fields

Ariel Pacetti

(joint work with J. Cremona and N. Vescovo)

Introduction

In this talk we present an alternative construction of tables of rational elliptic curves that can be used in some cases to construct elliptic curves over more general number fields, like imaginary quadratic ones. Nowadays the standard way to construct tables is via the use of modular symbols (as explained in [4]). It relies on the fact that all elliptic curves are modular, so it computes rational newforms, and the lattice attached to them. The advantage of such a method is that given a conductor N, it computes all curves of such conductor, but the disadvantage is that the dimension of the weight 2 modular forms space $S_2(\Gamma_0(N))$ grows linearly in N, while there are only few elliptic curves for each N.

The idea we use in our construction is the following: if K is a number field and

$$E : y^2 + a_1yx + a_3y = x^3 + a_2x^2 + a_4x + a_6$$

is an elliptic curve in Weierstrass model, the usual change of variables takes it into an equation of the form

$$E : y^2 = f(x) = x^3 + Ax^2 + Bx + C. \tag{1}$$

Then for constructing tables of elliptic curves it is enough to compute the possible polynomials $f(x)$. Note that the polynomial $f(x)$ is well defined up to translation (and the discriminant of $f(x)$ is translation invariant). Hence it is enough to compute all cubic polynomials of a given discriminant. The problem of computing cubic polynomials of bounded discriminant has been considered by many authors using the relation between cubic rings and binary cubic forms (see [1], [5] and the references therein), however none of them used such techniques for computing cubic polynomials whose discriminant is divisible by a specific set of primes. It is this issue that makes our approach more effective. We make use of the following new ideas to attack our problem:

- We give an algorithm using divisibility in the case where the polynomial is reducible.
- We consider curves up to twists, which in some cases gives a much better control on the relation conductor/discriminant.
- Finding the polynomial $f(x)$ is the same as finding a monogenous order $\mathscr{O}$ inside the ring of integers of the field $K[x]/f(x)$ (with the correct discriminant) and a generator for it. So we first construct all possible cubic extensions with prescribed ramification (in particular we first compute the 2-torsion of the possible elliptic curves) and then search for the orders $\mathscr{O}$ (and their generators).

Let K be a local field of residual characteristic different from 2 with uniformizer π, and E/K be an elliptic curve

$$E : y^2 = x^3 + a_2x^2 + a_4x + a_6.$$

Denote by E_π the twist by π of E, i.e. the curve

$$E_\pi : \pi y^2 = x^3 + a_2x^2 + a_4x + a_6.$$

The relation between the discriminants we search and the conductors is given by the following results/conjectures:

Lemma 0.1. *If E has potentially good reduction and $\pi \nmid 6$ then E or E_π has minimal discriminant valuation at π less than 6. We furthermore have*

$$v_\pi(\Delta(E)) = v_\pi(\Delta(E_p)) \pm 6.$$

Conjecture 1 (Szpiro's conjecture)**.** *Let K be a number field. Then for all $\epsilon > 0$, there exists a constant $C(K, \epsilon)$ such that any elliptic curve E/K of conductor $N(E)$ satisfies*

$$\mathscr{N}_{K/\mathbb{Q}}(\Delta(E)) \le C(K, \varepsilon)\mathscr{N}_{K/\mathbb{Q}}(N(E))^{6+\varepsilon}.$$

This conjecture remains rather elusive, the reader should note that it is equivalent to the ABC conjecture with exponent $\frac{3}{2}$ (see Proposition 11.5 of [8] for example). The best approximation currently available is to be found in [7] where the bound is exponential (instead of polynomial) in $N(E)$. Nevertheless, most curves satisfy Conjecture 1 (see [12] (1.15) page 488). Given a conductor $\mathfrak{n}$ we denote by $\mathfrak{n}^\infty$ the bound we get on the discriminant from Szpiro's conjectures.

1. Computing Curves with a two torsion point

Let us assume that K is imaginary quadratic. Furthermore, although it is not necessary, we assume it has class number 1 in order to make the exposition easier. Let E/K be an elliptic curve whose conductor divides $\mathfrak{n}^\infty$ and P be a 2-torsion point in $E(K)$. Translating the point to the origin we get an equation of the form

$$E : y^2 = f(x) = x(x^2 + ax + b), \tag{2}$$

with a and b algebraic integers, thus obtaining

$$\mathscr{D}(f) = b^2(a^2 - 4b). \tag{3}$$

Proposition 1.1. *Let E/K be an elliptic curve with a two torsion point. Then, up to twist, we can choose a model as before such that if $\mathfrak{p} \mid \mathfrak{n}$ and $\mathfrak{p} \mid a$ then $\mathfrak{p} \nmid b^2$. This choice makes the $\mathfrak{p}$-adic valuation of the discriminant minimal.*

Corollary 1.2. *Let E be an elliptic curve with a two torsion point as in* (3) *and with minimal discriminant among its twists as in the last Proposition. Let $\mathfrak{p}$ be a prime ideal such that $\mathfrak{p} \mid b$. Then one of the following must hold:*

- *$v_\mathfrak{p}(\Delta(E))$ is even and $v_\mathfrak{p}(b) = v_\mathfrak{p}(\Delta(E))/2$.*
- *$\mathfrak{p} \nmid 2$, $v_\mathfrak{p}(\Delta(E)) = 3$ and $v_\mathfrak{p}(b) = 1$.*
- *$\mathfrak{p} \mid 2$, $v_\mathfrak{p}(\Delta) \in \{4, 6, \dots, 2v_\mathfrak{p}(2) + 2, 2v_\mathfrak{p}(2) + 3\}$ and $v_\mathfrak{p}(b) = 1$.*

Remark 1.3 Note that once we know $\Delta(E)$, and b, there are two possible choices for the value of a (if such an integral square root exists), but both of them differ by the quadratic twist by χ_{-1}, so we take just one of them.

Given K, let $\mathcal{U}$ denote the units of $\mathscr{O}_K$. Recall that $\mathcal{U}$ is finite. Let $\{u_1, \dots, u_s\}$ be a set of representatives of $\mathcal{U}/(\mathcal{U})^6$.

Theorem 1.4. *Let $\mathfrak{n}$ be an square-free ideal in $\mathscr{O}_K$. Keeping the previous notation, the following algorithm computes all curves with a 2-torsion point whose conductor is supported at primes dividing $\mathfrak{n}$.*

1. *For each $\mathfrak{d} \mid \mathfrak{n}^\infty$, let $S_\mathfrak{d} = \{du_i : 1 \le i \le s\}$, where d is a generator of $\mathfrak{d}$, and u_i are as before.*
2. *For each $\Delta \in S_\mathfrak{d}$, search for all $b \in \mathscr{O}_K$ such that $b^2 \mid \Delta$ and b satisfies one of the conditions of Corollary 1.2.*
3. *Given Δ and b, check whether $\frac{\Delta}{b^2} + 4b$ is the square of an integer a, and in case it is, include the curve $y^2 = x^3 + ax^2 + bx$ to the list.*

2. Computing Curves without 2-torsion

Suppose now that f is monic and irreducible. Then $L := K[x]/f$ is a cubic extension of K unramified outside $\mathfrak{n}$, and $\mathscr{O}_K[x] \subset \mathscr{O}_L$ (the ring of integers of L) with

$$\mathscr{D}(f) = \mathscr{D}(\mathscr{O}_K[x]/f) = [\mathscr{O}_L : \mathscr{O}_K[x]]^2 \mathscr{D}(\mathscr{O}_L).$$

We compute the possible cubic extensions L using class field theory. Given L, let

$$D = \left\{ \mathfrak{d} \ : \ \mathfrak{d}^2 \mid \frac{\mathfrak{n}^\infty}{\mathscr{D}(\mathscr{O}_L)} \right\}.$$

Let $\mathscr{O} \subset \mathscr{O}_L$ be a suborder of index $\mathfrak{d} \in D$ which is monogenous, meaning $\mathscr{O} = \mathscr{O}_K[\alpha]$. Then the minimal polynomial $m_\alpha(x)$ of α gives a candidate for f, and all polynomials are obtained in this way. Then to compute the polynomials f we first compute all suborders $\mathscr{O}$ of a given index and then check whether they are monogenous. To do that, we use the relation between cubic orders and binary cubic forms (which is done in Delone-Faddeev). We denote by $F_{\mathscr{O}}$ the form attached to the order $\mathscr{O}$.

Proposition 2.1. *Let $\mathscr{O} \subset \mathscr{O}_L$ be an order and $\{1, \alpha, \beta\}$ a good basis for it. Then $\mathscr{O}$ is monogenous if and only if $F_{\mathscr{O}}(x, y)$ represents u_i for some $1 \leq i \leq s$. Furthermore, the generators of $\mathscr{O}$ (up to translation) are given by $\{A\alpha + B\beta\}$, where (A, B) varies through all the solutions of $F_{\mathscr{O}}(A, B) = u_i$.*

Theorem 2.2. *Given $\mathfrak{n}$ and assuming Conjecture 1, the following algorithm gives (up to twist) all the rational elliptic curves without 2-torsion whose conductor divides $2^8 \cdot \mathfrak{n}^6$.*

(1) Compute all cubic extensions L/K unramified outside $2\mathfrak{n}$.
(2) For each extension L, let $\mathscr{O}_L$ be its ring of integers and d_L denote its discriminant.
(3) For each $\mathfrak{d}$ such that $\mathfrak{d}^2 \mid \frac{\mathfrak{n}^\infty}{d_L}$, compute all primitive suborders $\mathscr{O} \subset \mathscr{O}_L$ of index $\mathfrak{d}$.
(4) For each $\mathscr{O}$, solve the Thue equation $F_{\mathscr{O}}(x, y) = u_i$ to get all generators $\gamma_{\mathscr{O}}$ of $\mathscr{O}$.
(5) Include the curve $y^2 = m_{\gamma_{\mathscr{O}}}(x)$ to the list.

References

[1] J.E. Cremona, *Reduction of binary cubic and quartic forms*, LMS J. Comput. Math. **2** (1999), 64–94.

[2] W.T. Gan and B. Gross and G. Savin, *Fourier coefficients of modular forms on G_2*, Duke Math. J. **115** (2002), 105–169.

[3] H. Cohen, *Advanced topics in computational number theory*, Graduate Texts in Mathematics, Springer-Verlag, New York, **193** (2000).

[4] J. E. Cremona, *Algorithms for modular elliptic curves*, Cambridge University Press, Cambridge, 2nd Ed. **32** (1997).

[5] K. Belabas and H. Cohen, *Binary cubic forms and cubic number fields*, Computational perspectives on number theory (Chicago, IL, 1995), AMS/IP Stud. Adv. Math., Amer. Math. Soc., Providence, RI **7** (1998), 191–219.

[6] The PARI Group, *PARI/GP version* 2.7.0, Bordeaux **32** (2014), available from http://pari.math.u-bordeaux.fr/.

[7] R. von Känel, *On Szpiro's discriminant conjecture*, Int. Math. Res. Not. IMRN **16** (2014), 4457–4491.

[8] J.H. Silverman, *The arithmetic of elliptic curves*, Graduate Texts in Mathematics, Springer, Dordrecht, 2nd Ed. **106** (2009).

[9] D.W. Masser, *Note on a conjecture of Szpiro*, Astérisque **183** (1990), 19–23.

[10] L. Szpiro, *Sur les propriétés numériques du dualisant relatif d'une surface arithmétique*, The Grothendieck Festschrift, Vol. III, Progr. Math., Birkhäuser Boston, Boston, MA **88** (1990), 229–246.

[11] M. Bennett and S. Yazdani, *A local version of Szpiro's conjecture*, Exp. Math. **21** (2012), 103–116.

[12] É. Fouvry, M. Nair and G. Tenenbaum, *L'ensemble exceptionnel dans la conjecture de Szpiro*, Bull. Soc. Math. France **120** (1992), 485–506.

[13] K. Ribet, *A modular construction of unramified p-extensions of$Q(\mu_p)$*, Invent. Math. **34** (1976), 151–162.

[14] B. Mazur, *How can we construct abelian Galois extensions of basic number fields?*, Bull. Amer. Math. Soc. (N.S.) **48** (2011), 155–209.

Gaussian summation

Hartmut Monien

Let $f : \mathbb{C} \to \mathbb{C}$ a complex valued function which is analytic close to the real half line $[1, \infty)$ and an asymptotic expansion at infinity in $1/z$ of the form

$$f(z) = \frac{a_2}{z^2} + \frac{a_3}{z^3} + \frac{a_4}{z^4} + \dots$$

with coefficients $a_n \in \mathbb{C}$. The problem of how to evaluate the sum $\sum_{n \geq 1} f(n)$ is ubiquitous. In the talk I gave a description of a new efficient method which is based on the following

Proposition. *For any f with the properties above the following identity holds*

$$\sum_{n \geq 1} f(n) = \int_C \psi\left(1 - z\right) f(z) dz$$

where the digamma function $\psi(z) = d\left(\Gamma(z)\right)/dz$ is the logarithmic derivative of the Euler Gamma function and the contour C is enclosing the real half line $[0, \infty)$.

Proof. The digamma function possesses only simple poles at every negative integer with residue one. □

Any rational approximation to the digamma function leads to an approximation for the summation. The theory of rational or Pade approximants is closely related to the moment problem and orthogonal polynomials. In the case under consideration the moments are given by zeta-values:

$$\mu_n = \int_C \frac{\psi\left(1 - z\right)}{z^2} \left(\frac{1}{z}\right)^n dz = \int_{C'} \psi\left(1 - \frac{1}{z}\right) z^n dz = \zeta(n + 2)$$

with $n \in \mathbb{N}_{>0}$ and the contour C' is taken around the real line $[0, 1]$.

Proposition. *The real Borel measure with support on the real line producing these moments is*

$$d\mu(x) = \sum_{k \geq 1} \frac{1}{k^2} \delta\left(x - \frac{1}{k}\right) dx \tag{1}$$

where $\delta(x)$ is the unit measure $x \in \mathbb{R}$.

Proof. Integrating x^n with the measure defined above. □

The monic orthogonal polynomials corresponding to the measure in (1) can then be expressed (see section 2.2 in [8]) as

$$p_n(z) = \frac{1}{H_n} \begin{vmatrix} \zeta(2) & \zeta(3) & \zeta(4) & \dots & \zeta(n+2) \\ \zeta(3) & \zeta(4) & \zeta(5) & \dots & \zeta(n+3) \\ \dots & \dots & \dots & \dots & \dots \\ \zeta(n+1) & \zeta(n+2) & \zeta(n+3) & \dots & \zeta(2n+1) \\ 1 & z & z^2 & \dots & z^n \end{vmatrix}$$

where $H_n = \det\left(\zeta(i+j)\right)_{1\le i,j\le n}$ are the Hankel determinants of the moments. The first few are given by

$$1, z - \frac{\zeta(2)}{\zeta(3)}, z^2 - \frac{\zeta(2)\zeta(5)-\zeta(3)\zeta(4)}{\zeta(2)\zeta(4)-\zeta(3)^2} z + \frac{\zeta(3)\zeta(5)-\zeta(4)^2}{\zeta(2)\zeta(4)-\zeta(3)^2}, \dots .$$

All orthogonal polynomials p_n obey a three term recursion:

$$p_{n+1}(x) = (x - a_n)p_n(x) + b_n p_{n-1}(x).$$

Determining the recursion coefficients for large n directly seems impossible because the discriminant of the resulting equation H_n tends to zero very quickly, e.g. $H_{100} \approx 4.9 \times 10^{-16684}$. The surprising experimental fact is that the coefficients a_n and b_n possess a surprisingly simple asymptotic behavior as $n \to \infty$:

$$\begin{aligned} a_n &= -\frac{1}{2n+1} + \frac{2}{(2n+1)^2} - \frac{7}{3}\frac{1}{(2n+1)^3} + \frac{16}{5}\frac{1}{(2n+1)^4} - \frac{41}{9}\frac{1}{(2n+1)^5} + \dots \\ b_n &= -\frac{1}{2n} - \frac{1}{(2n)^2} + \frac{2}{3}\frac{1}{(2n)^3} - \frac{6}{5}\frac{1}{(2n)^4} + \frac{56}{45}\frac{1}{(2n)^5} + \dots \end{aligned}$$

Once the recursion coefficients are known it is easy to determine the corresponding "Gaussian quadrature for sums" (see e.g. [6]). The method has been implemented in current development version `Pari/GP` as command *sumnummonien*. The remainder of the talk was devoted to the asymptotic behavior of the H_n. The obtain more detailed information about the polynomials and their zeros we are led to study the Hankel H_n. This can be done using tools from random matrix theory. The connection to random matrix theory is provided by the following result.

Proposition. *Let $F(s)$ be a Dirichlet series with coefficients $f(n)$, i.e.*

$$F(s) = \sum_{n\ge1} \frac{f(n)}{n^s}$$

The Hankel determinant $\det\left(F(i+j)\right)_{1\le i,j\le n}$ is given by

$$\det\left(F(i+j)\right)_{1\le i,j\le n} = \sum_{1\le m_1<m_2\ldots<m_n} \frac{f(m_1)f(m_2)\cdots f(m_n)}{(m_1m_2\ldots m_n)^{2n}} \prod_{i<j}(m_i-m_j)^2$$

Proof. The proof is purely combinatorial. Use identity (2.2.11) of [8] (see [5] for the origin of this identity) with the Borel measure of the proposition above. □

Corollary. *All determinants H_n are positive definite (see* [3, 4]*).*

Let $m = \{m_1, m_2, \ldots, m_n\}$ be a set of n positive integers. Let Λ be the set of (constrained) Borel measures

$$\Lambda_n = \left\{ \lambda \in \mathcal{M} \middle| d\lambda(x) = \frac{1}{n} \sum_{1 \leq j \leq n} \delta\left(x - \frac{m_j}{n}\right) dx \right\}$$

where $\delta(x)$ is the unit measure at x. The determinant can then be expressed as

$$H_n = \sum_{\lambda \in \Lambda_n} \exp\left(-n^2 \log(n) - n^2 \left(2 \int \log(x) d\lambda(x) - \iint \log|x-y| \, d\lambda(x) d\lambda(y)\right)\right).$$

To determine the leading asymptotics we are led to study the logarithmic potential problem for a *continous* constrained measure (see e.g. [1])

$$I[\lambda] = \inf\left\{ d\lambda \leq dx \middle| 2 \int \log(x) d\lambda(x) - \iint \log|x-y| \, d\lambda(x) d\lambda(y) \right\}.$$

Using methods from logarithmic potential theory I gave a proof that such a measure exists and is unique. It can be determined explicitly once its support has been determined [7, 2]. The constrained is exhausted for $x \in [0, 1/2]$ so that $d\lambda(x) = dx$. For $x > 1/2$

$$d\lambda(x) = \frac{2}{\pi} \left(\arctan\left(\frac{1}{\sqrt{2x-1}}\right) - \frac{\sqrt{2x-1}}{2x} \right) dx.$$

The leading asymptotic behavior of the Hankel determinants can be determined as

$$\log(H_n) = -n^2 \left(\log(2n) - \frac{3}{2}\right) + O\left(\frac{1}{n}\right).$$

References

[1] P. A. Deift, *Orthogonal polynomials and random matrices: a Riemann-Hilbert approach,* volume 3 of *Courant Lecture Notes in Mathematics.* New York University, Courant Institute of Mathematical Sciences, New York; American Mathematical Society, Providence, RI, 1999.

[2] P. D. Dragnev and E. B. Saff, *Constrained energy problems with applications to orthogonal polynomials of a discrete variable*, J. Anal. Math. **72** (1997), 223–259.

[3] F. Hausdorff, *Summationsmethoden und Momentfolgen. I*, Math. Z. **9(1-2)** (1921), 74–109.

[4] ———, *Summationsmethoden und Momentfolgen. II*, Math. Z. **9(3-4)** (1921), 280–299.

[5] E. Heine, *Handbuch der Kugelfunctionen. Theorie und Anwendungen. Band I, II*, Zweite umgearbeitete und vermehrte Auflage. Thesaurus Mathematicae, Physica-Verlag, Würzburg **1** (1961).

[6] H. Monien, *Gaussian quadrature for sums: a rapidly convergent summation scheme*, Math. Comp. **79(270)** (2010), 857–869.

[7] E.B. Saff and V. Totik, *Logarithmic potentials with external fields*, Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences] **316**, Springer-Verlag, Berlin, Appendix B by Thomas Bloom, (1997).

[8] G. Szegő, *Orthogonal polynomials*, American Mathematical Society, Providence, R.I., fourth edition, Colloquium Publications, **XXIII** (1975).

New Numerical Features in Pari/GP

Henri Cohen
(joint work with B. Allombert, K. Belabas and P. Molin)

The Pari/GP package is well-known for its ability to do sophisticated computations of an *arithmetical* nature, such as computing with number fields and elliptic curves, or finding linear relations between complex numbers with the `lindep` program. It is perhaps less known that it also has powerful *numerical* algorithms: to cite a few, many special functions (Bessel functions, confluent hypergeometric functions, incomplete gamma functions, elliptic functions, polylogarithms, etc...), the `sumalt` algorithm for summation of alternating series, the `intnum` doubly-exponential method for numerical integration, etc...

The aim of this talk was to present three new classes of numerical methods which have been implemented. At the time of the talk, they were available only in GIT branches (specifically `origin/master`, `origin/henri-zetamult`, and `origin/bill-Lfun`), but hopefully most of them should be soon in the main Pari distribution.

1. Integration, Summation, and Extrapolation

The first new package deals with numerical integration, summation, and extrapolation.

Concerning numerical integration: after numerous experiments at reasonable multiprecision accuracies (between 38 and 1000 decimal digits), the following conclusion has been reached: on *compact* intervals, there are two best methods: the doubly-exponential method (DEM), and Gauss–Legendre integration. The implementation of DEM has been considerably improved since the previous implementation, roughly by a factor of 3 or 4. Gauss–Legendre is very classical, but has proved to be by far the fastest method (sometimes 10 to 100 times faster) when it can be applied: DEM is quite robust, while Gauss–Legendre can easily not be applicable. On *noncompact* intervals such as $[a, \infty[$ or $]-\infty, \infty[$, only DEM is useful.

When Gauss–Legendre can be used, one can also easily compute *double integrals* quite fast: typically 0.1 second at 115 decimals.

Concerning numerical summation: once again there are two best methods: one is a variant of the Euler–MacLaurin summation formula which replaces derivatives by discrete analogues: this method is quite robust. The second method is due to H. Monien and so called the Gauss–Monien method: it is analogue to Gauss–Legendre but very clever, and similarly can be 10 to a 100 times faster when it can be applied, since it is much less robust.

Similarly, when Gauss–Monien can be used, one can easily compute double sums.

Finally, we also have implemented a method to compute limits and asymptotic expansions which was explained to us by D. Zagier.

2. Multizeta and Multipolylogs

The young Indian mathematician P. Akhilesh has devised a *very simple* algorithm for computing multizeta values (MZVs). Although such quantities have been computed for a very long time, for instance by D. Broadhurst and D. Zagier, Akhilesh's algorithm is very easy to implement, so is now part of `Pari/GP`. In addition, it has the advantage of being able to compute all MZVs of a given weight much faster than each one individually.

It is not difficult to generalize Akhilesh's algorithm to multipolylogs, at least in a certain domain of convergence, and this is also available.

3. The L-Function Package

The most important new feature in `Pari/GP` is the ability to compute with L-functions using some new ideas and improving old ones. The package is essentially divided into four independent parts.

- The computation of *inverse Mellin transforms* of gamma products. This uses basically the same ideas as T. Dokshitser's script and paper from 2002, but is highly optimized thanks to an estimate of the precise *conjectural* speed of convergence of the methods used. Note that contrary to Dokshitser's (and all other) packages, we do *not* need to compute generalized incomplete gamma functions, which are essential if one uses the approximate functional equation.
- The core program, based on ideas of A. Booker but put in the present form by P. Molin: a straighforward use of Poisson summation leads to a simple formula for computing L-function values for many arguments in terms of a *small* and *fixed* (of course depending on the desired accuracy) number of values of the corresponding theta function. The main difficulty resides in the precise estimate of the necessary parameters that are needed depending on the accuracy and the range of values of s for which one wants to compute $L(s)$.

  This part also includes programs for plotting and computing zeros on the critical line.
- The "guessing" programs: when only partial information is given on the L-function, we can compute (in order of difficulty) the root number, the polar part of the poles, the conductor, or the missing Euler factors. We can also check the functional equation if all the information is given.
- The "utility" programs for the most common types of L-functions. For instance, we may directly input:
  1. A polynomial or a number field: computes the Dedekind zeta function.
  2. An integer, representing a discriminant: computes the L-function of the corresponding quadratic character (the integer 1 corresponds to $\zeta(s)$).

(3) An elliptic curve, given either by its Cremona label or by a Weierstrass equation.
(4) A Hecke character, for the moment of finite order.
(5) An eta product, given as a 2-column factorization matrix.
(6) In complete generality, one can of course specify directly all the L-function data.

As a final remark, note that in the present implementation we assume that the L-function is "almost self-dual", i.e., that the functional equation is of the form $\Lambda(k-s) = w\overline{\Lambda(\overline{s})}$, but if two functions L_1 and L_2 are related by $\Lambda_1(k-s) = w\Lambda_2(s)$, we can simply use the package on $L_1 \pm wL_2$.

Local arithmetic of hyperelliptic curves

Tim Dokchitser

(joint work with V. Dokchitser, C. Maistret and A. Morgan)

Many fundamental arithmetic properties of a non-singular projective curve $C/\mathbb{Q}$ are encoded in its L-function and the associated invariants:

$$\begin{array}{lcll} L(C,s) & = & \prod_p \frac{1}{F_p(p^{-s})} & L\text{-function}, \\ N & = & \prod_p p^{n_p} & \text{conductor}, \\ w & = & w_\infty \prod_p w_p & \text{root number}. \end{array}$$

These are all products of local invariants at primes p, and these local invariants all come from the l-adic representation

$$H^1_{\text{ét}}(C_{\bar{\mathbb{Q}}_p}, \mathbb{Q}_l)$$

of the absolute Galois group $\text{Gal}(\bar{\mathbb{Q}}_p/\mathbb{Q}_p)$. The question is how to compute this representation for a given curve $C/\mathbb{Q}$ at a given prime p. When C has good reduction at p, this is classical — the representation is unramified, and the characteristic polynomial of Frobenius comes from counting points on the reduced curve.

We would like to understand what happens at bad primes p, and the case we consider is that of hyperelliptic curves and $p \neq 2$. The question is entirely local, so say we have a curve C/K over a local field K:

$$C : y^2 = c \prod_{r \in R} (x - r), \qquad R \subset \bar{K}.$$

The degree of the equation $n = |R|$ is $2g+1$ or $2g+2$, where g is the genus of C. Write v for the valuation on $\bar{K}$, normalized so that $v : K \twoheadrightarrow \mathbb{Z}$.

It is not surprising that the shape of the Galois representation has to do with the combinatorics of the roots R, to be precise, with their pairwise p-adic distances. Define a *cluster* s as a non-empty subset of roots R which is cut out by a disc,

$$s \;=\; R \cap \{x \in \bar{K} \mid v(x-\alpha) < \beta\}.$$

Call the smallest such β the *depth* d_s, and write $s' < s$ for an inclusion of maximal subclusters. Call a cluster *principal* if

(1) $|s| > 2$,
(2) s does not contain a subcluster $s' \lneq s$ of size $\geq 2g$,
(3) $s \neq R$ when $R = s_1 \coprod s_2$ is a union of two subclusers of odd size.

Our first result is a criterion for when C has semistable reduction over K:

Theorem 1 (Semistability). *A curve C of genus $g \geq 2$ is semistable over K if and only if (a) the ramification degree of $K(R)$ over K is at most 2, and (b) every principal cluster s has $d_s \in \mathbb{Z}$ and*

$$\nu_s := v(c) + \sum_{r \in R \setminus s} v(r - s) + |s| d_s \ \in \ 2\mathbb{Z}.$$

Next, we describe the $\mathrm{Gal}(\bar{K}/K)$-representation $H^1_{\text{ét}}(C_{\bar{K}}, \mathbb{Q}_l)$. It has dimension $2g$, and it decomposes

$$H^1_{\text{ét}}(C_{\bar{K}}, \mathbb{Q}_l) = V_{ab} \oplus (V_t \otimes \mathrm{Sp}_2),$$

with V_{ab} the *abelian part*, V_t the *toric part* and $\mathrm{Sp}(2)$ the 'standard' 2-dimensional (non-semisimple) representation.

For a cluster s write s_0 for the set of odd maximal subclusters $s' < s$. Call s *even* if $|s|$ is even and $s_0 \neq \emptyset$, and *übereven* if $|s|$ is even and $s_0 = \emptyset$.

Theorem 2 (Toric part). *As a $\mathrm{Gal}(\bar{K}/K)$-module,*

$$V_t = \begin{cases} \mathbb{Q}_l[\textit{even clusters}] & \textit{if } R \textit{ is not übereven}, \\ \ker(\mathbb{Q}_l[\textit{even clusters}] \xrightarrow{\Sigma} \mathbb{Q}_l) & \textit{if } R \textit{ is übereven}, \end{cases}$$

where $\mathbb{Q}_l[...]$ is viewed as a signed permutation representation. (There is a natural signed permutation action of $\mathrm{Gal}(\bar{K}/K)$ on even clusters.)

As for the abelian part, to describe it completely, even in the good reduction case, one needs to involve some point counting on the reduced curves. For simplicity, to give a closed form expression, we describe it as an inertia module, i.e. a representation of the inertia subgroup $I_{\bar{K}/K}$ of $\mathrm{Gal}(\bar{K}/K)$.

Theorem 3 (Abelian part). *As an $I_{\bar{K}/K}$-module,*

$$V_{ab} = \bigoplus_{\substack{I_K \text{ orbits of} \\ \text{clusters } s,\ |s| \geq 3}} \mathrm{Ind}^{I}_{\mathrm{Stab}s}(V_s \ominus \epsilon_s),$$

with $V_s = (\mathbb{Q}_l[s_0] \ominus \mathbf{1}) \otimes$explicit 1-dimensional character, and $\epsilon_s = 0$ if $|s_0|$ is odd, and $\epsilon_s = \det V_s$ if $|s_0|$ is even.

The above theorems will be implemented in Magma in full generality soon, and are already used to compute invariants of hyperelliptic curves over local fields, and their L-functions and global conductors over $\mathbb{Q}$ and over number fields.

Computing elliptic curves of fixed conductor

Michael Bennett
(joint work with A. Rechnitzer)

We discussed new, old and older still methods for computing elliptic curves with bad reduction outside given sets of primes. Applying these, we are now able to find models for all elliptic curves over the rationals with prime conductor bounded by 10^{10} and, conjecturally, by 10^{12}. We then mention extensions of these results to the case of more general conductors and to curves over number fields.

The main technique involved is appeal to classical invariant theory to reduce the problem to one of solving Thue equations, typically of the form $F(x, y) = 8$ for binary cubic forms of discriminant $\pm 4p$.

Kodaira dimension of certain orthogonal modular varieties

Anthony Várilly-Alvarado
(joint work with S. Tanimoto)

A very general point on the coarse moduli space of smooth complex cubic fourfolds $\mathcal{C}$ gives rise to a cubic fourfold X that does not harbor many algebraic surfaces: the integral Hodge conjecture is known to hold for X [12], and the intersection $A(X) := \mathrm{H}^{2,2}(X) \cap \mathrm{H}^4(X, \mathbb{Z})$ is spanned by h^2 for such X, where h is the restriction of the hyperplane section in $\mathbb{P}^5$ to X. Motivated by the search of provably rational cubic fourfolds [1], Hassett [6] initiated the systematic study of the Noether-Lefschetz locus $\{X \in \mathcal{C} : \mathrm{rk}(A(X)) > 1\}$ of $\mathcal{C}$. He showed this locus is the union of a countable number of divisors $\mathcal{C}_d$ parametrizing special cubic fourfolds. A cubic fourfold X is special, of discriminant d, if $A(X)$ contains a rank 2 saturated lattice of algebraic cycles $K_d = \langle h^2, T \rangle$ of (unsigned) discriminant d.

Very little is known about the geometry of the Noether-Lefschetz divisors $\mathcal{C}_d$. We know that $\mathcal{C}_d$ is not empty if and only if $d > 6$ and $d \equiv 0$ or $2 \bmod 6$, and it is irreducible if nonempty [6, Theorem 1.0.1]. We study Kodaira dimension of $\mathcal{C}_d$. Work of Hassett [6] and Nuer [10] shows that $\mathcal{C}_d$ has negative Kodaira dimension for $d = 6n + 2$ and $1 \leq n \leq 7$, as well as for $d = 6n$ and $2 \leq n \leq 6$. Through a connection with moduli spaces of polarized K3 surfaces [6, §5], we also know that a sparse but infinite set of $\mathcal{C}_d$'s are of general type, because the corresponding moduli of K3 surfaces are of general type [2]. We determine the Kodaira dimension for all but a few $\mathcal{C}_d$.

Theorem ([11]). *Let $\mathcal{C}_d \subseteq \mathcal{C}$ be the moduli space of special cubic fourfolds possessing a labeling of discriminant d.*

(1) Assume that $d = 6n + 2$ for some integer n.

(a) If $n > 18$ and $n \notin \{20, 21, 25\}$ then $\mathcal{C}_d$ is of general type;

[1] It is believed that a very general cubic fourfold is not rational, but no examples of nonrational cubic fourfolds are known as of this writing.

   (b) If $n > 13$ and $n \neq 15$ then $\mathcal{C}_d$ has nonnegative Kodaira dimension.

(2) Assume that $d = 6n$ for some integer n.

   (a) If $n > 18$ and $n \notin \{20, 22, 23, 25, 30, 32\}$ then $\mathcal{C}_d$ is of general type;

   (b) If $n > 16$ and $n \notin \{18, 20, 22, 30\}$ then $\mathcal{C}_d$ has nonnegative Kodaira dimension.

Remark. *A remarkable recent result of Ma* [8] *implies, among other things, that $\mathcal{C}_d$ is of general type for $d \equiv 2 \bmod 6$ and $d \gg 0$, although no explicit bound for how large d would have to be is given.*

The proof of our theorem uses the full force of work Gritsenko, Hulek and Sankaran [2, 3, 4, 5]. We start with the observation that $\mathcal{C}_d$ is birational to a modular variety of orthogonal type. Let $L := K_d^{\perp}(-1)$ denote the orthogonal complement of the lattice K_d in $(+1)^{\oplus 21} \oplus (-1)^{\oplus 2} \simeq \mathrm{H}^4(X, \mathbb{Z})$, with its pairing multiplied by -1. It is an even lattice of signature $(2, 19)$. Let

$$\mathcal{D}_L = \{[x] \in \mathbb{P}(L \otimes \mathbb{C}) : (x, x) = 0, (x, \bar{x}) > 0\}^+$$

be one of the two components the period domain associated to L. Then there is a subgroup Γ of finite index in $O^+(L)$ such that $\mathcal{C}_d$ is birational to $\Gamma \backslash \mathcal{D}_L$.

This observation enables us to apply the "low-weight cusp form trick" of Gritsenko, Hulek, and Sankaran, which reduces the proof of our theorem to constructing a single cusp form of weight < 19 with respect to Γ vanishing along the ramification divisor of the modular projection $\pi\colon \mathcal{D}_L \to \Gamma \backslash \mathcal{D}_L$. An idea of Kondo [7], brought to maturity in [2, 5] shows that a modification of a modular form introduced by Borcherds [1] supplies the needed cusp form, provided one can find a primitive embedding of L into the Borcherds lattice $L_{2,26} := U^{\oplus 2} \oplus E_8(-1)^{\oplus 3}$ in such a way that L is orthogonal to at least two, but no more than twelve elements of $L_{2,26}$ of norm -2. This embedding problem is the focal point of our work.

References

[1] R. E. Borcherds, *Automorphic forms on* $\mathrm{O}_{s+2,2}(\mathbf{R})$ *and infinite products*, Invent. Math. **120** (1995), 161–213.

[2] V. A. Gritsenko, K. Hulek and G. K. Sankaran, *The Kodaira dimension of the moduli of K3 surfaces*, Invent. Math. **169** (2007), 519–567.

[3] ———, *Moduli spaces of irreducible symplectic manifolds*, Compos. Math. **146** (2010), 404–434.

[4] ———, *Moduli spaces of polarized symplectic O'Grady varieties and Borcherds products*, J. Differential Geom. **88** (2011), 61–85.

[5] ———, *Moduli of K3 surfaces and irreducible symplectic manifolds*, Hand book of moduli. Vol. I, Adv. Lect. Math. (ALM) **1**, (2013), 459–526.

[6] B. Hassett, *Special cubic fourfolds*, Compositio Math. **120** (2000), 1–23.

[7] S. Kondō, *On the Kodaira dimension of the moduli space of K3 surfaces. II*, Compositio Math. **116** (1996), 111–117.

[8] S. Ma, *Finiteness of stable orthogonal modular varieties of non-general type*, (2013), Preprint, `arXiv:1309.7121`.

[9] K. McKinnie J. Sawon, S. Tanimoto, and A. Várilly-Alvarado , *Brauer groups on K3 surfaces and arithmetic applications*, (2014), Preprint, `arXiv:1404.5460`.

[10] H. Nuer, *Unirationality of moduli spaces of special cubic fourfolds and K3 surfaces*, (2015), Preprint, arXiv:1503.05256.

[11] S. Tanimoto and A. Várilly-Alvarado, *Kodaira dimension of moduli of moduli of special cubic fourfolds*, (2015), Preprint.

[12] C. Voisin, *Some aspects of the Hodge conjecture*, Jpn. J. Math. **2** (2007), 261–296.

Hurwitz Belyi maps

David Roberts

Belyi maps. Any degree n function F from a Riemann surface X to the Riemann sphere P^1 has $2n+2\,\text{genus}(\mathsf{X})-2$ critical points in X, counting multiplicity. Generically, the critical points $x_i \in \mathsf{X}$ are distinct, and the the critical values $F(x_i) \in \mathsf{P}^1$ are also distinct. The map F is called a Belyi map if its critical values are within $\{0, 1, \infty\}$. So Belyi maps are as far from generic as possible, and moreover their critical values are normalized.

We say that a degree n Belyi map β is *full* if its monodromy group is A_n or S_n. A full Belyi map, with $n \geq 4$ to remove non-trivial automorphisms of the map, has a well-defined minimal number field $K \subset \mathbb{C}$ over which it has a canonical model. Assuming that $K = \mathbb{Q}$, the map also has a well-defined set of primes $\mathcal{P}$ at which it has bad reduction. To illustrate these notions, define $\beta : \mathsf{P}^1 \to \mathsf{P}^1$ by

$$\beta(x) = \frac{(x+2)^9 x^{18}(x^2-2)^{18}(x-2)}{(x+1)^{16}(x^3-3x+1)^{16}}. \tag{1}$$

Then β is indeed a Belyi map. Its monodromy group is S_{64}, its field of definition is visibly $\mathbb{Q}$, and its set of bad primes is $\mathcal{P} = \{2, 3\}$.

For $\mathcal{P}$ a finite set of primes, let $N(\mathcal{P})$ be the set of degrees $n \geq 4$ for which there exists a full Belyi map defined over $\mathbb{Q}$ with bad reduction set within $\mathcal{P}$. One knows that $N(\emptyset) = \emptyset$ and we expect that for any prime p, one has $N(\{p\}) = \emptyset$ as well. The largest degree n we know of in $N(\{p_1, p_2\})$ with $p_1, p_2 \leq 13$ is 64, coming from (1). In general, it seems hard to construct large degrees in $N(\mathcal{P})$ by direct elementary methods.

Hurwitz covers. There is however a promising indirect method for constructing large degrees in $N(\mathcal{P})$ for certain $\mathcal{P}$ as follows. Let $h = (G, C, \nu)$ be a Hurwitz parameter, meaning a triple where G be a finite group, $C = (C_1, \ldots, C_s)$ is a list of distinct non-identity classes, and $\nu = (\nu_1, \ldots, \nu_s)$ is a list of positive integers satisfying $\prod C_i^{\nu_i} = 1$ in the abelianization G^{ab}. Then there is a corresponding unramified covering of complex algebraic varieties

$$\pi_h : \mathsf{Hur}_h \to \mathsf{Conf}_\nu. \tag{2}$$

Here the base Conf_ν is the space of tuples $(D_1, \ldots, D_s)$ of disjoint subsets of P^1 with $|D_i| = \nu_i$. The cover Hur_h is a classical Hurwitz moduli space. The degree of the cover π_h is called a Hurwitz number, and these Hurwitz numbers are complicated and much studied quantities. In a large regime this degree is given by the approximate formula

$$n_h \approx \frac{|G^{\mathrm{ab}}|}{|G|^2} \prod_{j=1}^{s} |C_i|^{\nu_i}. \tag{3}$$

In fact, when sufficiently many C_i are present then the approximation (3) is exact.

Two classical facts about Hurwitz covers are particularly relevant for us. First, when all the classes C_i are rational, then the cover (2) are defined over $\mathbb{Q}$. Second, the bad reduction set $\mathcal{P}_h$ of (2) is contained within the set of primes dividing $|G|$. More recently, with Venkatesh we considered monodromy groups in the setting of fixed (G, C) and sufficiently large $\min \nu_i$. We found necessary and sufficient conditions for the monodromy group to be A_{n_h} or S_{n_h}. The main condition for this fullness is that G is appropriately close to being a nonabelian simple group.

Definition of Hurwitz-Belyi maps. A Belyi pencil of type ν is an embedding

$$u : \mathsf{P}^1 - \{0,1,\infty\} \to \mathsf{Conf}_\nu. \tag{4}$$

Given a Hurwitz parameter $h = (G, C, \nu)$ and a Belyi pencil of type ν, the corresponding Hurwitz Belyi map $\beta_{h,u}$ is obtained by by pulling back and canonically completing:

$$\begin{tikzcd}
\mathsf{X} \arrow[r, phantom, "\supset"] \arrow[d, "\beta_{h,u}"'] & \mathsf{X}^0 \arrow[r] \arrow[d] & \mathsf{Hur}_h \arrow[d, "\pi_h"] \\
\mathsf{P}^1 \arrow[r, phantom, "\supset"] & \mathsf{P}^1 - \{0,1,\infty\} \arrow[r, "u"] & \mathsf{Conf}_\nu.
\end{tikzcd}$$

Suppose both (2) and (4) are defined over $\mathbb{Q}$. with respective bad reduction sets $\mathcal{P}_h$ and $\mathcal{P}_u$. Then the Hurwitz Belyi map $\beta_{h,u} : \mathsf{X} \to \mathsf{P}^1$ is defined over $\mathbb{Q}$ with bad reduction within $\mathcal{P}_h \cup \mathcal{P}_u$.

Explicit examples of Belyi pencils defined over $\mathbb{Q}$ include

$$\begin{array}{rcl}
u_4 : \mathsf{P}^1_j - \{0,1,\infty\} & \to & \mathsf{Conf}_{3,1}, \\
j & \mapsto & ((t^3 - 3jt + 2j), \{\infty\}), \\
u_5 : \mathsf{P}^1_j - \{0,1,\infty\} & \to & \mathsf{Conf}_{4,1}, \\
j & \mapsto & (((j-1)^2 t^4 - 6j(j-1)t^2 - 8j(j-1)t - 3j^2), \{\infty\}).
\end{array}$$

Associated polynomial discriminants are

$$\begin{array}{rcl}
D_4(j) & = & 2^2 3^3 j^2 (j-1), \\
D_5(j) & = & -2^{12} 3^3 j^4 (j-1)^6.
\end{array}$$

So the bad reduction sets are $\mathcal{P}_{u_4} = \mathcal{P}_{u_5} = \{2,3\}$. There is no fullness assumption associated to (4), and so it is easy to get rational Belyi pencils into infinitely many Conf_ν, all with bad reduction set say $\{2\}$.

Unboundedness conjecture. Say that a finite set $\mathcal{P}$ of primes is *anabelian* if it contains the set of primes dividing a nonabelian finite simple group. For example, the classification of finite simple groups says that the anabelian $\mathcal{P}$ with $|\mathcal{P}| \leq 3$ are exactly $\{2, 3, p\}$ with $p \in \{5, 7, 13, 17\}$.

Given an anabelian $\mathcal{P}$, there are infinitely many full π_h defined over $\mathbb{Q}$ with bad reduction within $\mathcal{P}$. By specialization one gets infinitely many Belyi maps $\beta_{h,u}$ defined over $\mathbb{Q}$ with bad reduction within $\mathcal{P}$. Braid group computations indicate that there is no general tendency for monodromy groups to become smaller under specialization. Accordingly, we expect the following:

Conjecture. *Let $\mathcal{P}$ be an anabelian set of primes. Then $N(\mathcal{P})$ is infinite.*

This conjecture is a direct geometric analog of an arithmetic conjecture made with Venkatesh for number fields. In this earlier conjecture, we specialized Hurwitz covers to suitable points in Conf_ν. Here we are specializing the same covers, but now to suitable curves in Conf_ν. Our hope is that the new conjecture may be easier to prove, because confirmation of fullness upon specialization can now be done by braid group computations.

Note that for any G, the numbers of the form (3) have density zero. While there is not much evidence either way, we think that the most likely scenario is that $N(\mathcal{P})$ always has density zero, and is finite when $\mathcal{P}$ is not anabelian.

Examples. Four similar examples of full Hurwitz Belyi maps are as follows, with bad reduction set $\mathcal{P} = \{2, 3, 5\}$ for the first two and $\mathcal{P} = \{2, 3, 7\}$ for the last two:

#	h	u	n_h	$(\lambda_0, \lambda_1, \lambda_\infty)$	N
1	$(S_5, (41, 2111), (3, 1))$	u_4	32	$(3^{10}\,1^2,\ 2^{16}, 10\ 6\ 5\ 4^2\ 3)$	10
2	$(A_6, (3111, 2211), (4, 1)$	u_5	192	$(3^{64},\ 2^{84}\,1^{24}, 15^3\ 12^5\ 9^3\ 6^8\ 5\ 4\ 3)$	10^{33}
3	$(G_2(2), (2B, 4D), (3, 1)$	u_4	40	$(3^{12}\,4,\ 2^{20}, 12\ 8^2\ 7\ 3\ 2)$	10^4
4	$(GL_3(2), (22111, 331), (4, 1))$	u_5	96	$(3^{32}, 2^{40}1^{16}, 21^2 9^3 7^1 6^3 2)$	10^{15}

In all cases, the covering curve has genus zero and an explicit rational function $f(x)/g(x)$ analogous to our initial example (1) is obtained. In Example 1, the constituents are

$$\begin{aligned} f(x) &= -\left(x^{10} - 38x^9 + 591x^8 - 4920x^7 + 24050x^6 - 71236x^5 + 125638x^4 \right. \\ &\qquad \left. -124536x^3 + 40365x^2 + 85050x - 91125\right)^3 \left(x^2 - 14x - 5\right), \\ g(x) &= 2^{20}3^3x^6(x-5)^5\left(x^2 - 4x + 5\right)^4 (x-9)^3. \end{aligned}$$

In general, the partitions λ_0, λ_1, and λ_∞ come from the factorizations of $f(x)$, $f(x) - g(x)$, and $g(x)$ respectively.

Our initial example had $(\lambda_0, \lambda_1, \lambda_\infty) = (18^3\,9\,1,\ 8\,1^{56},\ 16^4)$. It was one of $N = 35$ full Belyi maps with these invariants, the others being conjugate via a common degree 34 abstract field of definition with discriminant

$$2^{71}3^{44}5^{27}7^{27}11^{23}13^{19}19^{15}23^{10}29^{11}31^{8}37^{4}47^{3}.$$

In our four examples, one would expect from (3) applied to the Hurwitz parameter $(A_{n_h}, (\lambda_0, \lambda_1, \lambda_\infty), (1, 1, 1))$ approximately N full coverings with these invariants. While the one we present is rational, it seems possible that all the others are likewise conjugate to each other, with almost all primes less than n_h ramified in their common field of definition.

Some References

This talk is in the process of becoming *Hurwitz Belyi maps.*

The initial degree 64 example is $U_{8,9}$ from *Chebyshev covers and exceptional number fields* on my homepage.

The full-monodromy theorem with Venkatesh is Theorem 5.1 in *Hurwitz monodromy and full number fields,* Algebra and Number Theory 9 (2015), no. 3, 511-545. The unboundedness conjecture for number fields is also in this paper.

A standard reference on Hurwitz schemes is Bertin and Romagny, *Champs de Hurwitz* Mém. Soc. Math. Fr. 125–126 (2011), 219pp.

Example 4 takes as its starting point Theorem 4.2 from Gunter Malle, *Multiparameter polynomials with given Galois group*, J. Symbolic Comput. 30 (2000) 717–731.

Braid group computations in higher degree should be feasible using Magaard, Shpectorov, Völklein, *A GAP package for braid orbit computation and applications.* Experiment. Math 12 (2003), no. 4, 385–393.

Braid computations after specialization to Belyi pencils will involve ideas from Jordan Ellenberg. *Galois invariants of dessins d'enfants.* 27-42, Proc. Sympos. Pure Math., 70 (2002).

On ranks of elliptic curves over complex function fields

Douglas Ulmer

If k is a finite field and E is an elliptic curve over $K = k(t)$ with $j(E)$ not in k, then there are finite extensions of K of the form $L = k(u)$ (or $L = k'(u)$ with k'/k finite) such that the analytic rank of E over L is arbitrarily large. Our goal in this talk is to show that the situation is completely different when $K = \mathbb{C}(t)$. More precisely, for a 'very general' elliptic curve over $\mathbb{C}(t)$ of height at least 3, and for L a finite extension of K of the form $K = \mathbb{C}(u)$, we have $E(\mathbb{C}(u)) = 0$.

The theorem can be reformulated as saying that a very general elliptic fibration $E \to \mathbb{P}^1$ over $\mathbb{C}$ with Kodaira dimension 1 has no rational curves other than the zero section and components of singular fibers. We present a heuristic explanation of why this should be true. We also sketch a proof that proceeds by showing that if the theorem is false, then the rational curves in question fit together into an algebraic family which in a certain sense is determined by one 'universal' rational curve. This leads to a contradiction.

Returning to the heuristic, we note that it suggests that for any elliptic fibration $\mathcal{E}$ over $\mathbb{P}^1$ over $\mathbb{C}$ of Kodaira dimension 1, the degrees over the base of rational curves on $\mathcal{E}$ are bounded above. This fits beautifully with a conjecture of Lang on rational curves on surfaces of general type, and we end by formulating a general conjecture and explaining a consequence for ranks of elliptic curves in towers of complex function fields.

On reduced Arakelov divisors of a number field

Tran Nguyen Thanh Ha

Let F be a number field. The Arakelov class group Pic_F^0 of F is an analogue of the Picard group of a curve. From this group one can 'read off' the class number h_F and the regulator of F. A good tool to compute Pic_F^0 is the class of reduced Arakelov divisors of F. In the first part, we recall the definitions of Arakelov divisors and the Arakelov class group of a number field and its structure. In the second part, we first discuss 'nice' properties of reduced Arakelov divisors. Then we generalize the concept of reduced Arakelov divisors and introduce C–reduced divisors for a given number $C \geq 1$ as well as their properties. Finally we show one of its applications: computing the functions h^0 for number fields with unit groups of rank at most 2.

References

[1] E. Bayer-Fluckiger, *Lattices and number fields*, Algebraic geometry: Hirzebruch 70 (Warsaw, 1998) **241** (1994), 69–84.

[2] J. Buchmann, *A subexponential algorithm for the determination of class groups and regulators of algebraic number fields*, Séminaire de Théorie des Nombres, Paris 1988–1989 **91** (1990), 27–41.

[3] J. Buchmann and H.C. Williams, *On the infrastructure of the principal ideal class of an algebraic number field of unit rank one*, Mathematics of Computation **50** (1988), 569–579.

[4] P. Francini, *The size function h^0 for quadratic number fields*, J. Théor. Nombres Bordeaux **13** (2001), 125–135.

[5] P. Francini, *The size function h° for a pure cubic field*, Acta Arith. **111** (2004), 225–237.

[6] R.P. Groenewegen, *An arithmetic analogue of Clifford's theorem*, J. Théor. Nombres Bordeaux **13** (2001), 143–156.

[7] A. K. Lenstra, and H. W. Lenstra, and L. Lovász, *Factoring polynomials with rational coefficients*, Math. Ann. **261** (1982), 515–534.

[8] H. W. Lenstra, *On the calculation of regulators and class numbers of quadratic fields*, Number theory days, 1980 (Exeter, 1980) **56** (1982), 123–150.

[9] H. W. Lenstra, *Algorithms in algebraic number theory*, Bull. Amer. Math. Soc. (N.S.) **26** (1992), 211–244.

[10] H. W. Lenstra, *Lattices*, Algorithmic number theory: lattices, number fields, curves and cryptography, Math. Sci. Res. Inst. Publ. **44** (2008), 127–181.

[11] R. Schoof, *Quadratic fields and factorization*, Computational methods in number theory, Part II, Math. Centre Tracts, **155** (1982), 235–286.

[12] R. Schoof, *Computing Arakelov class groups*, Algorithmic number theory: lattices, number fields, curves and cryptography, Cambridge Univ. Press, Cambridge **44** (2008), 447–495.

[13] D. Shanks, *The infrastructure of a real quadratic field and its applications*, Proceedings of the Number Theory Conference (Univ. Colorado, Boulder, Colo.) (1972), 217–224.

[14] G. van der Geer and R. Schoof, *Effectivity of Arakelov divisors and the theta divisor of a number field*, Selecta Math. (N.S.) **6** (2000), 377–398.

Heuristics for distributions of Arakelov class groups

Alex Bartel
(joint work with H. Lenstra)

Often, when a mathematical object is drawn in some "random" manner, the probability that it is isomorphic to a given object A is inversely proportional to $\#\operatorname{Aut} A$. The Cohen–Lenstra heuristics [1, 2], which make predictions on the distribution of class groups of "random" algebraic number fields, may be seen as a special case of this rule, provided that one passes to Arakelov class groups. But to make sense of this rigorously, one needs to be able to compare sizes of automorphism groups, even when those are infinite. Concretely, if F is a number field, then the Pontryagin dual of the Arakelov class group is an extension of the form

$$1 \to \mathrm{Cl}_F^{\vee} \to (\mathrm{Pic}_F^0)^{\vee} \to \mathrm{Hom}(\mathcal{O}_F^{\times}, \mathbb{Z}) \to 1,$$

where $-^{\vee}$ denotes the Pontryagin dual $\mathrm{Hom}_{\mathrm{cts}}(-, \mathbb{R}/\mathbb{Z})$. If F is Galois, then the above is an exact sequence of Galois modules. In order to conceptually explain the behaviour of ideal class groups in families, one would like to make sense of expressions like $\frac{\#\operatorname{Aut}(\mathrm{Pic}^0_{F_1})^{\vee}}{\#\operatorname{Aut}(\mathrm{Pic}^0_{F_2})^{\vee}}$, where F_1 and F_2 are suitable Galois number fields.

Our main results, formulated as Theorems 1 and 2 below, express that, for certain pairs of modules L and M over certain types of ring, one can meaningfully define the ratio of the size of the automorphism group $\operatorname{Aut} M$ of M to the size of $\operatorname{Aut} L$, even when their orders $\#\operatorname{Aut} M$ and $\#\operatorname{Aut} L$ are infinite. If $\operatorname{Aut} L$ can be naturally embedded in $\operatorname{Aut} M$ as a subgroup of finite index, then the ratio mentioned may be defined to be that index. Our approach consists of defining such an index in a more general situation, and only dependent on the isomorphism classes of L and M. We shall write $\mathrm{ia}(L, M)$ for the "index of automorphism groups" that we define.

Denote by $\mathbb{Z}$ the ring of integers, by $\mathbb{Q}$ the field of rational numbers, by $\mathbb{Q}_{>0}$ the multiplicative group of positive rational numbers, by $R[G]$ the group ring of a group G over a ring R, and by $(G : H)$ the index of a subgroup H of a group G. By "module" we shall always mean "left module".

Theorem 1. *Let G be a finite group, let V be a finitely generated $\mathbb{Q}[G]$-module, and put*

$$\mathcal{S} = \{L : L \text{ is a finitely generated } \mathbb{Z}[G]\text{-module with } \mathbb{Q}\otimes_{\mathbb{Z}} L \cong V \text{ as } \mathbb{Q}[G]\text{-modules}\}.$$

Then there exists a unique function $\mathrm{ia}\colon \mathcal{S} \times \mathcal{S} \to \mathbb{Q}_{>0}$ such that

(a) if L, L', M, $M' \in \mathcal{S}$ and $L \cong L'$, $M \cong M'$, then $\mathrm{ia}(L, M) = \mathrm{ia}(L', M')$;
(b) if L, M, $N \in \mathcal{S}$, then $\mathrm{ia}(L, M) \cdot \mathrm{ia}(M, N) = \mathrm{ia}(L, N)$;
(c) if $M \in \mathcal{S}$, and $L \subset M$ is a submodule of finite index, then letting $H = \{\sigma \in \operatorname{Aut} M : \sigma L = L\}$ and $\rho\colon H \to \operatorname{Aut} L$ map $\sigma \in H$ to $\sigma|_L$, one has

$$\mathrm{ia}(L, M) = \frac{(\operatorname{Aut} M : H) \cdot \#\ker \rho}{(\operatorname{Aut} L : \rho H)}.$$

To explain part (c), we remark that it is not hard to show that one has $L \in \mathcal{S}$ and that the three cardinal numbers $(\operatorname{Aut} M : H)$, $\#\ker\rho$, $(\operatorname{Aut} L : \rho H)$ are finite. Since these three numbers may be thought of as the ratio of the sizes of $\operatorname{Aut} M$ and H, of H and ρH, and of $\operatorname{Aut} L$ and ρH, respectively, one may think of the expression in (c) as the ratio of the sizes of $\operatorname{Aut} M$ and $\operatorname{Aut} L$. The same argument shows that one has indeed $\operatorname{ia}(L, M) = (\#\operatorname{Aut} M)/\#\operatorname{Aut} L$ if $\operatorname{Aut} M$ and $\operatorname{Aut} L$ are finite.

As an example, let G be the trivial group, and put $n = \dim_{\mathbb{Q}} V$. Then each $L \in \mathcal{S}$ is isomorphic to the direct sum of $\mathbb{Z}^n$ with a finite abelian group L_0, and $\operatorname{Aut} L$ is isomorphic to a semidirect product $\operatorname{Hom}(\mathbb{Z}^n, L_0) \rtimes (\operatorname{Aut} L_0 \times \operatorname{GL}(n, \mathbb{Z}))$, where both $\operatorname{Hom}(\mathbb{Z}^n, L_0)$ and $\operatorname{Aut} L_0$ are finite. Writing $M \in \mathcal{S}$ similarly, and "cancelling" $\operatorname{GL}(n, \mathbb{Z})$, one is led to believe that

$$\operatorname{ia}(L, M) = \frac{\#\operatorname{Hom}(\mathbb{Z}^n, M_0) \cdot \#\operatorname{Aut} M_0}{\#\operatorname{Hom}(\mathbb{Z}^n, L_0) \cdot \#\operatorname{Aut} L_0} = \frac{(\# M_0)^n \cdot \#\operatorname{Aut} M_0}{(\# L_0)^n \cdot \#\operatorname{Aut} L_0}.$$

Making this informal argument rigorous, one discovers that if a function ia as in Theorem 1 exists, it must be given by the formula just stated. However, that this formula does define a function meeting all conditions, in particular (c), is not obvious. Likewise, for general G the uniqueness statement of Theorem 1 is easy by comparison to the existence statement.

We give an entirely algebraic proof of Theorem 1, obtaining the theorem as a special case of a much more general result, of which the formulation requires some terminological preparation.

Isogenies. A *group isogeny* is a group homomorphism $f \colon H \to G$ such that $\#\ker f < \infty$ and $(G : fH) < \infty$, and its *index* $\operatorname{i}(f)$ is defined to be equal to $(G : fH)/\#\ker f$. For a ring R, an *R-module isogeny* is an R-module homomorphism that is an isogeny as a map of additive groups. A *ring isogeny* is a ring homomorphism that is an isogeny as a map of additive groups. The index of an isogeny of one of the latter two types is the index of the induced group isogeny on the additive groups.

Commensurabilities. If X, Y are objects of a category $\mathcal{C}$, then a *correspondence* from X to Y in $\mathcal{C}$ is a triple $c = (Z, f, g)$, where Z is an object of $\mathcal{C}$ and $f \colon Z \to X$ and $g \colon Z \to Y$ are morphisms in $\mathcal{C}$; we will often write $c \colon X \rightleftharpoons Y$ to indicate a correspondence. A *group commensurability* is a correspondence $c = (Z, f, g)$ in the category of groups for which both f and g are isogenies, and the *index* $\operatorname{i}(c)$ of such an isogeny is defined to be $\operatorname{i}(g)/\operatorname{i}(f)$. For a ring R, one defines R-module commensurabilities and their indices analogously, replacing the category of groups by the category of R-modules. Likewise, one defines ring commensurabilities and their indices.

Endomorphisms and automorphisms. Let R be a ring, and let

$$c = (N, f, g) \colon L \rightleftharpoons M$$

be a correspondence of R-modules. We define the *endomorphism ring* $\operatorname{End} c$ of c to be the subring $\{(\alpha, \beta, \gamma) \in (\operatorname{End} L) \times (\operatorname{End} N) \times (\operatorname{End} M) : \alpha f = f\beta,\ \gamma g = g\beta\}$

of the product ring $(\operatorname{End} L) \times (\operatorname{End} N) \times (\operatorname{End} M)$. There are natural ring homomorphisms $\operatorname{End} c \to \operatorname{End} L$ and $\operatorname{End} c \to \operatorname{End} M$ sending (α, β, γ) to α and γ, respectively; we shall write $\mathrm{e}(c)\colon \operatorname{End} L \rightleftharpoons \operatorname{End} M$ for the ring correspondence consisting of $\operatorname{End} c$ and those two ring homomorphisms. Similarly, writing $E^\times$ for the multiplicative group of invertible elements of a ring E, we define the *automorphism group* $\operatorname{Aut} c$ of c to be the group $(\operatorname{End} c)^\times$, and we write $\mathrm{a}(c) : \operatorname{Aut} L \rightleftharpoons \operatorname{Aut} M$ for the group correspondence consisting of $\operatorname{Aut} c$ and the natural maps $\operatorname{Aut} c \to \operatorname{Aut} L$, $\operatorname{Aut} c \to \operatorname{Aut} M$.

Theorem 2. *Let Z be an infinite domain such that for all non-zero $m \in Z$ the ring Z/mZ is finite, let Q be the field of fractions of Z, let A be a semisimple Q-algebra of finite vector space dimension over Q, let $R \subset A$ be a sub-Z-algebra with $Q \cdot R = A$, and let L, M be finitely generated R-modules. Then:*

(a) there is an R-module commensurability $L \rightleftharpoons M$ if and only if the A-modules $Q \otimes_Z L$ and $Q \otimes_Z M$ are isomorphic;

(b) if $c\colon L \rightleftharpoons M$ is an R-module commensurability, then $\mathrm{e}(c)\colon \operatorname{End} L \rightleftharpoons \operatorname{End} M$ *is a ring commensurability, and* $\mathrm{a}(c) : \operatorname{Aut} L \rightleftharpoons \operatorname{Aut} M$ *is a group commensurability;*

(c) if c, $c' : L \rightleftharpoons M$ are R-module commensurabilities, then one has

$$\mathrm{i}(\mathrm{e}(c)) = \mathrm{i}(\mathrm{e}(c')), \quad \mathrm{i}(\mathrm{a}(c)) = \mathrm{i}(\mathrm{a}(c')).$$

Part (c) is the essential statement of Theorem 2. It shows that one can define $\mathrm{ia}(L, M) = \mathrm{i}(\mathrm{a}(c))$, independently of c, if one has $Q \otimes_Z L \cong_A Q \otimes_Z M$ and $c\colon L \rightleftharpoons M$ is an R-module commensurability. One deduces the existence part of Theorem 1 from Theorem 2 by putting $Z = \mathbb{Z}$, $Q = \mathbb{Q}$, $A = \mathbb{Q}[G]$, and $R = \mathbb{Z}[G]$.

Note that parts (b) and (c) of Theorem 2 are also trivially true if Z is finite, since the assumptions then imply that the endomorphism rings of L, M are finite, and $\mathrm{i}(\mathrm{e}(c)) = \frac{\#\operatorname{End} M}{\#\operatorname{End} L}$ for any commensurability $c : L \rightleftharpoons M$.

When one applies this theory of commensurability to dual Arakelov class groups of number fields, the story takes a surprising twist. If G is a fixed finite group, and p is a prime nor dividing $2|G|$, then we postulate that in suitable families of number fields F, $\mathbb{Z}_p \otimes_{\mathbb{Z}} (\mathrm{Pic}^0_F)^\vee$ behaves like a "random" $\mathbb{Z}_p[G]$-module with the expected probability weights. We show that this is in fact equivalent to the original Cohen–Lenstra heuristic. But we *prove* that the obvious global conjecture, predicting the behaviour of $\mathbb{Z}\left[\frac{1}{2|G|}\right] \otimes_{\mathbb{Z}} (\mathrm{Pic}^0_F)^\vee$ is false, because there is interesting interplay between the Galois module structure of the class group and the unit group. To find the most general correct heuristic is work in progress.

References

[1] H. Cohen and H.W. Lenstra, Jr., *Heuristics on class groups of number fields*, Number theory, Noordwijkerhout 1983, Lecture Notes in Math., **1068** (1984), 33–62, Springer, Berlin.

[2] H. Cohen and J. Martinet, *Étude heuristique des groupes de classes des corps de nombres*, J. Reine Angew. Math., **404** (1990), 39–76.

A heuristic for boundedness of ranks of elliptic curves

John Voight

(joint work with Jennifer Park, Bjorn Poonen and Melanie Matchett Wood)

Let $E\colon y^2 = x^3 + Ax + B$ be an elliptic curve over $\mathbb{Q}$ with $A, B \in \mathbb{Z}$ and such that there is no prime ℓ with $\ell^4 \mid A$ and $\ell^6 \mid B$. Then A, B are determined by the isomorphism class of E over $\mathbb{Q}$ and every elliptic curve over $\mathbb{Q}$ appears in this form. We define the height of E to be $\mathrm{ht} E = \max(|4A^3|, |27B^2|)$. Let $\mathcal{E}_{\leq H} = \{E : \mathrm{ht}\, E \leq H\}$ for $H > 0$.

Question. Let $r \in \mathbb{Z}_{\geq 0}$ and p be prime. Ranging over finite abelian p-groups G equipped with a nondegenerate alternating pairing $[\ ,\ ]$, what is the probability

$$\begin{aligned}&\mathrm{Prob}((\text{Ш}(E)[p^\infty], \langle\ ,\ \rangle) \simeq (G, [\ ,\ ]) \mid \mathrm{rk}\, E(\mathbb{Q}) = r)\\ &\quad = \lim_{H\to\infty} \frac{\#\{E \in \mathcal{E}_{\leq H} : (\text{Ш}(E)[p^\infty], \langle\ ,\ \rangle) \simeq (G, [\ ,\ ]) \,\mathrm{and}\, \mathrm{rk} E(\mathbb{Q}) = r\}}{\#\{E \in \mathcal{E}_{\leq H} : \mathrm{rk} E(\mathbb{Q}) = r\}}\ ?\end{aligned}$$

A first answer to this question is given by Delaunay [2, 3], in analogy with the Cohen–Lenstra heuristics for class groups. He predicts (counting by conductor, instead of height) that the answer to this question is given by the probability

$$\mathrm{Prob}_{\mathcal{D}_r}(G, [\ ,\ ]) = \frac{\#G^{1-r}}{\#\,\mathrm{Aut}(G, [\ ,\ ])} \prod_{i \geq r+1} (1 - p^{1-2i}),$$

where $\mathrm{Aut}(G, [\ ,\ ])$ denotes the group of automorphisms of G that respect the pairing.

A second answer is given by work of Bhargava, Kane, Lenstra, Poonen, and Rains [1]. If $A \in M_n(\mathbb{Z}_p)_{\mathrm{alt}}$, then there is a natural nondegenerate alternating pairing $\langle\ ,\ \rangle_A$ on the finite abelian group $\mathrm{coker}(A : \mathbb{Z}_p^n \to \mathbb{Z}_p^n)_{\mathrm{tors}}$. For all n satisfying $n \equiv r \pmod 2$, there is a natural probability measure on the set

$$\{A \in M_n(\mathbb{Z}_p)_{\mathrm{alt}} : \mathrm{rk}_{\mathbb{Z}_p}(\ker A) = r\},$$

and we let $\mathcal{A}_{n,r}(G, [\ ,\ ])$ be the measure of

$$\{A \in M_n(\mathbb{Z}_p)_{\mathrm{alt}} : \mathrm{rk}_{\mathbb{Z}_p}(\ker A) = r \text{ and } ((\mathrm{coker}\, A)_{\mathrm{tors}}, \langle\ ,\ \rangle_A) \simeq (G, [\ ,\ ])\}.$$

Then the measures $\mathcal{A}_{n,r}$ converge to a probability measure $\mathcal{A}_r$. This model is also consistent with many known properties of the arithmetic of elliptic curves.

Theorem ([1], Theorems 1.6(c) and 1.10(b))**.** *The probability measures $\mathcal{D}_r$ and $\mathcal{A}_r$ coincide.*

Let $X(H), \eta(H) \to \infty$ as $H \to \infty$ to be calibrated later; we insist now only that X grows rapidly in comparison to η. Our basic model is as follows. For $E/\mathbb{Q}$ with $\mathrm{ht}\, E = H$, we choose $n \in \lfloor \eta(H) \rfloor + \{0, 1\}$ uniformly at random and

$$A \in M_n(\mathbb{Z})_{\mathrm{alt}, \leq X(H)} = \{A \in M_n(\mathbb{Z}) : A^t = -A \text{ with entries in } [-X(H), X(H)] \cap \mathbb{Z}\}$$

uniformly at random. Then we predict that

$$(\operatorname{coker} A)_{\mathrm{tors}} \text{ models } Ш(E) \text{ and } \operatorname{rk}(\ker\ A) \text{ models } \operatorname{rk} E(\mathbb{Q})$$

as $H \to \infty$.

This model predicts that $\operatorname{rk}(E) = 0, 1, \geq 2$ with probabilities $50\%, 50\%, 0\%$. For $r = 0, 1$, by equidistribution of $\mathbb{Z}$ in $\mathbb{Z}_p$ we recover the predicted probability measure $\mathcal{A}_r$ as above.

To predict ranks, we combine two ingredients. The first is a theorem which counts the number of matrices, based on work of Eskin–Katznelson [4].

Theorem. *If $1 \leq r \leq n-4$ and $n-r$ is even, then*

$$\#\{A \in M_n(\mathbb{Z})_{\mathrm{alt},\leq X} : \operatorname{rk}(\ker A) \geq r\} \asymp_n X^{n(n-r)/2}.$$

Since $\#M_n(\mathbb{Z})_{\mathrm{alt},\leq X} \asymp_n X^{n(n-1)/2}$, we predict that for $E \in \mathcal{E}_{\leq H}$,

$$\operatorname{Prob}(\operatorname{rk} E(\mathbb{Q}) \geq r) \asymp \operatorname{Prob}(\operatorname{rk}(\ker A) \geq r) \asymp \frac{X^{n(n-r)/2}}{X^{n(n-1)/2}} = (X^{-n/2})^{r-1}.$$

Second, we calibrate the model.

Conjecture. *We have* $\underset{E \in \mathcal{E}_{\leq H}}{\operatorname{Average}} L(E, 1) \overset{?}{\asymp} 1$ *as* $H \to \infty$.

This conjecture is true in quadratic twist families. Let

$$Ш_0(E) := \begin{cases} \#Ш(E), & \text{if } \operatorname{rk} E(\mathbb{Q}) = 0; \\ 0, & \text{if } \operatorname{rk} E(\mathbb{Q}) > 0. \end{cases}$$

Then

$$L(E, 1) \overset{?}{=} Ш_0(E)\Omega_E(\operatorname{ht} E)^{o(1)}$$

according to the conjecture of Birch–Swinnerton-Dyer.

Lemma. *We have*

$$(\operatorname{ht} E)^{-1/12} \ll \Omega_E \ll (\operatorname{ht} E)^{-1/12} \log(\operatorname{ht} E)$$

so $\Omega = H^{-1/12+o(1)}$.

Together, these two statements imply

$$\underset{E \in \mathcal{E}_{\leq H}}{\operatorname{Average}}\, Ш_0(E) = H^{-1/12+o(1)}$$

as $H \to \infty$. On the other hand,

$$\underset{A \in M_n(\mathbb{Z})_{\mathrm{alt},\leq X}}{\operatorname{Average}} |\det A| \asymp X^n.$$

So we calibrate

$$X(H)^{\eta(H)} = H^{1/12+o(1)}.$$

We then predict that

$$\operatorname{Prob}(\operatorname{rk} E(\mathbb{Q}) \geq r) \overset{?}{=} (X^{-n/2})^{r-1} = H^{-(r-1)/24+o(1)}$$

for $E \in \mathcal{E}_{\le H}$. We have $\#\mathcal{E}_{\le H} \asymp H^{5/6} = H^{20/24}$, so

$$\sum_{E \in \mathcal{E}_{\le H}} (\operatorname{ht} E)^{-(r-1)/24} = H^{(21-r)/24+o(1)}, \text{ for } 1 \le r \le 21$$

and the sum converges for $r > 21$. So we predict (in agreement with a heuristic of Watkins–Granville [5, Section 11]):

- All but finitely many elliptic curves E over $\mathbb{Q}$ satisfy $\operatorname{rk} E(\mathbb{Q}) \le 21$; and
- $\#\{E \in \mathcal{E}_{\le H} : \operatorname{rk} E \ge r\} = H^{(21-r)/24+o(1)}$.

References

[1] M. Bhargava, D. M. Kane, H. W. Lenstra, B. Poonen, and E. Rains, *Modeling the distribution of ranks, Selmer groups, and Shafarevich-Tate groups of elliptic curves*, (2013), Preprint, arXiv:1304.3971v2.

[2] C. Delaunay, *Heuristics on Tate-Shafarevich groups of elliptic curves defined over* $\mathbb{Q}$, Experiment. Math. **10** (2001), 191–196.

[3] C. Delaunay, *Heuristics on class groups and on Tate-Shafarevich groups: the magic of the Cohen-Lenstra heuristics*, Ranks of elliptic curves and random matrix theory, London Math. Soc. Lecture Note Ser., Cambridge Univ. Press, Cambridge **341** (2007), 323–340.

[4] A. Eskin and Yonatan R. Katznelson, *Singular symmetric matrices: Computing other invariants of topological spaces of dimension three*, Duke Math. J. **79** (1995), 515–547.

[5] M. Watkins, S. Donnelly, N. D. Elkies, T. Fisher, A. Granville, and N. F. Rogers, *Ranks of quadratic twists of elliptic curves*, (2014), to appear in *Publications mathématiques de Besançon*, available at http://magma.maths.usyd.edu.au/~watkins/papers/RANK7.pdf

Databases of elliptic curves over $\mathbb{Q}$ and rank distributions

Wei Ho

(joint work with J. Balakrishnan, N. Kaplan, S. Spicer, W. Stein and J. Weigandt)

In joint work in progress with J. Balakrishnan, N. Kaplan, S. Spicer, W. Stein, and J. Weigandt, we have created several databases of elliptic curves over $\mathbb{Q}$, ordered by notions of "naive height," and computed arithmetic invariants like the rank and 2-Selmer groups for each curve (conditional on standard conjectures like GRH, BSD, and parity). Many previous databases, such as that of Stein-Watkins and Cremona, consist of elliptic curves with relatively low conductor (instead of height). Our interest in making such a database developed because of theoretical results on Selmer groups and ranks of elliptic curves ordered by height. In addition, it is easy to enumerate all curves up to a given height (but not up to a given conductor).

One database consists of elliptic curves in short Weierstrass form

$$E : y^2 = x^3 + Ax + B$$

with $A, B \in \mathbb{Z}$, where the height of such a curve E is $\max\{|A|^3, B^2\}$. This database contains all $18,562,150$ integral elliptic curves with height up to 10^8 (we only take one curve for each isomorphism class). The average rank of these curves is approximately 0.899, which is slightly higher than the current best known theoretical upper bound of Bhargava-Shankar. (Most experts believe that the average rank, in the limit, will be 0.5 because of parity and the belief that the proportion of curves with rank ≥ 2 will be negligible).

We also have a database of $100,000$ elliptic curves in short Weierstrass form with coefficients in $\mathbb{Z}$ and height between 10^{14} and 2×10^{14}; these were randomly selected from all curves with those height restrictions. The average rank of these $100,000$ curves is approximately 0.821, and there are indeed proportionally fewer rank 2 curves in this database as opposed to the first (13.8% versus 17.3%). The decrease in rank 2 curves is expected by various heuristics (Watkins, Granville, Park-Poonen-Voight-Wood).

Other databases in progress include those with marked points, such as elliptic curves with one marked point of the form

$$E : y^2 + a_3 y = x^3 + a_2 x^2 + a_4 x,$$

where the height of such a curve is $\max\{a_2^6, a_3^4, |a_4|^3\}$. For the 3594891 isomorphism classes of such curves with integral coefficients and height up to 10^8, we find that the average rank is approximately 1.832. As expected, the distributions of ranks is similar to that of the short Weierstrass curves except shifted up by 1 in rank.

The proportion of plane cubic curves with a rational point

Tom Fisher

We consider plane cubic curves $C = \{F(x, y, z) = 0\} \subset \mathbb{P}^2$ where F is a ternary cubic (i.e. homogeneous polynomial of degree 3) with integer coefficients. We write $H(F)$ for the maximum of the absolute values of the coefficients of F. For $\mathcal{P}$ a property of ternary cubics we let

$$\rho(\mathcal{P}, B) = \frac{\#\{ \text{ ternary cubics } F \text{ with } H(F) \leq B \text{ satisfying } \mathcal{P} \ \}}{\#\{ \text{ ternary cubics } F \text{ with } H(F) \leq B \ \}}.$$

It has been shown by Bhargava, Cremona and Fisher [2] that the proportion of cubics which are everywhere locally soluble (ELS) is

$$\lim_{B \to \infty} \rho(\text{ELS}, B) = c = 0.97256076...$$

where c is given explicitly as a product over primes. Bhargava [1] has shown that the proportion that are soluble over $\mathbb{Q}$ satisfies

$$\liminf_{B \to \infty} \rho(\text{SOLUBLE}, B) > 0 \quad \text{and} \quad \limsup_{B \to \infty} \rho(\text{SOLUBLE}, B) < c,$$

and he conjectures that

$$\lim_{B \to \infty} \rho(\text{SOLUBLE}, B) = \tfrac{1}{3}c. \tag{1}$$

We report on an experiment to test this conjecture numerically. For each $B \in \{10, 30, 100, 300, 1000\}$ we picked 1000 ternary cubics, with coefficients chosen uniformly at random from $[-B, B] \cap \mathbb{Z}$. The numbers which were soluble or everywhere locally soluble (ELS) were as follows.

B	#SOLUBLE	#ELS
10	802	972
30	$683 - 687$	972
100	$562 - 602$	969
300	$454 - 578$	975
1000	$285 - 599$	977

In all except the first experiment (with $B = 10$) we were not able to determine the number of soluble cubics exactly, but have instead shown (under GRH) that the total lies in the range indicated.

As should be expected for plane cubics chosen at random, all the plane cubics in our experiment are smooth. Moreover the Jacobian elliptic curve $E/\mathbb{Q}$ has trivial torsion subgroup, and in all but one example (with $B = 10$) it is the only elliptic curve in its isogeny class. In all but about 1.5% of cases, the discriminant of the ternary cubic (a degree 12 polynomial in the coefficients) is equal to the minimal discriminant of E. Since there is no good reason for the discriminant to have repeated factors, the conductor of E is of roughly the same size, that is, of order B^{12}.

If $C/\mathbb{Q}$ is an everywhere locally soluble plane cubic with Jacobian $E/\mathbb{Q}$, then we write $[C]$ for its class in the 3-Selmer group $S^{(3)}(E/\mathbb{Q})$. We have

$$C(\mathbb{Q}) \neq \emptyset \iff [C] \in \operatorname{im}(\delta)$$

where δ is the connecting map in the Kummer exact sequence

$$0 \longrightarrow E(\mathbb{Q})/3E(\mathbb{Q}) \xrightarrow{\delta} S^{(3)}(E/\mathbb{Q}) \longrightarrow \text{Ш}(E/\mathbb{Q})[3] \longrightarrow 0. \tag{2}$$

The map δ may be realised as follows. Given $P \in E(\mathbb{Q})$ let f_1, f_2, f_3 be a basis for the Riemann Roch space $\mathcal{L}(4(0_E) - (P))$. The image of the morphism $E \to \mathbb{P}^2$ given by $(f_1 : f_2 : f_3)$ is a plane cubic C. Then $\delta(P) = [C]$. In Magma [3] this cubic is computed using the function `GenusOneModel(3,P)`. In conjunction with the function `IsEquivalent` for testing equivalence of ternary cubics, this gives a convenient way of reducing the problem of deciding whether $C(\mathbb{Q}) \neq \emptyset$ to that of finding generators for $E(\mathbb{Q})$. When $C(\mathbb{Q}) \neq \emptyset$ we also obtain an explicit point, and indeed this may be read off from the second returned arguments.

The methods we used to compute $E(\mathbb{Q})$ were as follows. All the functions described are in Magma, the most recent addition being the implementation of the Cassels-Tate pairing due to Donnelly. Our descriptions are slightly simplified by the fact $E(\mathbb{Q})_{\mathrm{tors}} = 0$.

- We ran `TwoDescent` on $E/\mathbb{Q}$ to give a list of $2^{r_2}-1$ binary quartics, representing the non-zero elements of the 2-Selmer group $S^{(2)}(E/\mathbb{Q})$. This involves computing the class group and units for a degree 3 number field, and it is here that our results are conditional on GRH. The 2-Selmer rank r_2 is an upper bound for $\operatorname{rank} E(\mathbb{Q})$.
- We ran `CasselsTatePairing` on all pairs of binary quartics computed in the previous step. This gives an alternating pairing on $S^{(2)}(E/\mathbb{Q})$ whose kernel, of size 2^{r_4}, is the image of $S^{(4)}(E/\mathbb{Q})$. The 4-Selmer rank r_4 is again an upper bound for $\operatorname{rank} E(\mathbb{Q})$.
- We ran `FourDescent` on all binary quartics passing the test in the previous step. This produces a list of $2^{r_2-1}(2^{r_4}-1)$ quadric intersections representing the inverse pairs of elements of order 4 in $S^{(4)}(E/\mathbb{Q})$. We then ran `PointSearch` on each of these 4-coverings. Whenever we find a rational point we map it down to E, thus potentially improving our lower bound for $\operatorname{rank} E(\mathbb{Q})$. In all unresolved cases we searched on the 4-coverings up to height 10^{10}.
- In some of the more difficult cases we ran `CasselsTatePairing` on pairs consisting of a binary quartic and a quadric intersection. Let S_2 be the image of $S^{(4)}(E/\mathbb{Q}) \to S^{(2)}(E/\mathbb{Q})$. If $\xi, \eta \in S_2$, say with $\xi' \mapsto \xi$ and $\eta' \mapsto \eta$ then there is an alternating pairing

  $$S_2 \times S_2 \to \mathbb{F}_2 \; ; \quad (\xi, \eta) \mapsto \langle \xi', \eta \rangle_{\mathrm{CT}} = \langle \xi, \eta' \rangle_{\mathrm{CT}}$$

  whose kernel, of size 2^{r_8}, is the image of $S^{(8)}(E/\mathbb{Q})$. The 8-Selmer rank r_8 is again an upper bound for $\operatorname{rank} E(\mathbb{Q})$. Unfortunately in many of the cases with $B = 1000$, `CasselsTatePairing` did not finish in reasonable time, and so we were not yet able to determine r_8.

In the unresolved cases, the discriminant and conductor of E were too large for there to be much hope of using 3-descent, 8-descent, 9-descent, L-values or Heegner points. We were nonetheless able to make use of 12-descent.

If $C_3 \to E$ and $C_4 \to E$ are 3- and 4-coverings of E, then the fibre product $C_{12} = C_3 \times_E C_4$ is a 12-covering of E. A practical way to compute equations for C_{12}, in a way suitable for point searching, is described in [5], and implemented in `TwelveDescent`. We ran this function with C_3 the original plane cubic C, and C_4 running over a set of representatives for $S^{(4)}(E/\mathbb{Q})$. In cases where $C(\mathbb{Q}) \neq \emptyset$ this often helped in finding a rational point. However when $C(\mathbb{Q}) = \emptyset$ this does not help in finding generators for $E(\mathbb{Q})$, and so does not help in proving that $C(\mathbb{Q}) = \emptyset$. In all unresolved cases we searched on the 12-coverings up to height 10^{24}. In a few cases we let C_3 run over the subgroup of $S^{(3)}(E/\mathbb{Q})$ generated by C and the image of the points already known in $E(\mathbb{Q})$. This helped us find the second generator for some of the rank 2 curves.

Some of the points we found have quite large height. The following table relates to those cubics in each experiment where we were successful in finding a rational point. The height of $P = (x : y : z)$ is $H(P) = \max(|x|, |y|, |z|)$ where x, y, z are coprime integers. We indicate the distribution of $\log H(P)$ by the percentiles below. For example, in the experiment with $B = 1000$, in 40% of the cases where we found a rational point, this point P had $\log H(P) \leq 34.3$. We went to some effort to make sure that the rational points analysed here are the rational points of smallest height on each cubic, but we have not proved this.

B	0%	10%	20%	30%	40%	50%	60%	70%	80%	90%	100%
10	0.0	0.0	0.0	0.0	0.0	0.7	1.1	1.9	3.1	6.3	74.8
30	0.0	0.0	0.7	1.1	1.9	2.9	4.4	6.7	11.9	30.0	265.6
100	0.0	0.7	2.7	4.2	6.7	9.9	15.2	23.6	42.3	84.3	300.6
300	0.0	3.3	7.4	12.8	19.2	29.6	45.0	70.5	116.8	206.6	340.4
1000	0.0	4.6	12.0	20.6	34.3	56.4	90.9	131.4	214.1	289.9	367.8

Delaunay conjectures [4, Section 6.2] that for elliptic curves of rank r the average size of $\text{Ш}(E/\mathbb{Q})[3]$ is $1+1/3^{2r-1}$. So by (2) the proportion of non-identity elements in $S^{(3)}(E/\mathbb{Q})$ that are in the image of δ is

$$\gamma_r = \frac{3^r - 1}{3^r(1 + 1/3^{2r-1}) - 1} = \frac{3^r - 1}{3^r - 1 + 1/3^{r-1}} = \begin{cases} 0 & \text{if } r = 0 \\ 2/3 & \text{if } r = 1 \\ 24/25 & \text{if } r = 2 \end{cases}$$

Bhargava's heuristic [1] suggests that, among everywhere locally soluble ternary cubics with Jacobian of rank r, the proportion with a rational point should be γ_r. The reason for discounting the identity element, is that when ternary cubics are ordered by height, 0% of them have a rational point of inflection. Indeed in our experiment, just four of the cubics with $B = 10$ and one with $B = 30$ had a rational point of inflection. (It happens that these were all examples with $r > 0$.)

The following table gives an analysis of our results broken down by rank of the Jacobian. For this purpose, we assume the parity conjecture, so that if an elliptic curve is shown by descent to have rank at most n, and we have found at least $n-1$ independent points, then we assume it has rank n. In a few cases we were still unable to determine whether the rank is n or $n - 2$. We have included the totals for these cases in brackets in the column for rank n.

	rank $E(\mathbb{Q})$	0	1	2	3	4	5	6	Total
$B = 10$	#ELS	112	308	338	164	46	4	0	972
	# soluble	0	253	335	164	46	4	0	802
	# unresolved	0	0	0	0	0	0	0	0
$B = 30$	#ELS	158	374	300(+1)	109	25	4	1	972
	# soluble	0	269	275	109	25	4	1	683
	# unresolved	0	3	0(+1)	0	0	0	0	4
$B = 100$	#ELS	267	377	226(+1)	77	19	2	0	969
	# soluble	0	249	215	77	19	2	0	562
	# unresolved	0	39	0(+1)	0	0	0	0	40
$B = 300$	#ELS	290	477	153(+4)	46	5	0	0	975
	# soluble	0	257	146	46	5	0	0	454
	# unresolved	0	119	1(+4)	0	0	0	0	124
$B = 1000$	#ELS	307	496	115(+31)	25(+2)	1	0	0	977
	# soluble	0	154	103	25(+2)	1	0	0	285
	# unresolved	0	277	6(+31)	0	0	0	0	314

If one admits the conjecture of Katz-Sarnak-Goldfeld that 50% of elliptic curves have rank 0 and 50% have rank 1, then one arrives at the factor $(\gamma_0 + \gamma_1)/2 = 1/3$ in the conjecture (1). It is clear from our data that the convergence to the expected proportions γ_r is happening rather faster than the convergence to the expected rank distribution.

Acknowledgments

I would like to thank Manjul Bhargava, Kiran Kedlaya and Don Zagier for useful comments following the talk.

References

[1] M. Bhargava, A positive proportion of plane cubics fail the Hasse principle, `http://arxiv.org/abs/1402.1131`.

[2] M. Bhargava, J.E. Cremona and T.A. Fisher, The proportion of plane cubic curves that everywhere locally have a point, to appear in *Int. J. Number Theory.*

[3] W. Bosma, J. Cannon and C. Playoust, The Magma algebra system I: The user language, *J. Symbolic Comput.* **24**, 235–265 (1997).

[4] C. Delaunay and F. Jouhet, p^ℓ-torsion points in finite abelian groups and combinatorial identities, *Adv. Math.* **258** (2014), 13–45.

[5] T.A. Fisher, Finding rational points on elliptic curves using 6-descent and 12-descent, *Journal of Algebra* 320 (2008), **2**, 853–884.

Point counting in average polynomial time: an update

David Harvey

1. Introduction

Let $F(x) \in \mathbb{Z}[x]$ be a squarefree polynomial of degree $2g+1$ or $2g+2$. For all but finitely many odd primes p, the equation $y^2 = F(x) \pmod p$ defines a hyperelliptic curve X_p of genus g over $\mathbb{F}_p$.

We are interested in efficient algorithms for computing $Z_p(T)$, the zeta function of X_p. All complexity bounds below refer to deterministic bit complexity. Schoof's algorithm and its generalisations [1, 7, 8] obtain $Z_p(T)$ in time $(\log p)^{O(g^2 \log g)}$, which is polynomial in $\log p$ for fixed g, but grows rapidly with g. Kedlaya's algorithm [6] computes $Z_p(T)$ in time $g^{4+\epsilon} p^{1+\epsilon}$, which is polynomial in g but exponential in $\log p$. A major open question is whether it is possible to compute $Z_p(T)$ in time polynomial in both g and $\log p$.

The author recently proved a partial result in this direction [2]: given a prescribed bound N, one may compute $Z_p(T)$ simultaneously for all primes $p < N$ in time $g^{8+\epsilon} N (\log N)^{3+\epsilon}$, provided that N is large enough relative to g and to the size of the coefficients of F. Thus the average time per prime is $g^{8+\epsilon}(\log p)^{4+\epsilon}$, which is polynomial in g and $\log p$.

It is unclear whether the algorithm of [2] is practical, but the techniques introduced in that paper were used by the author and Sutherland [4, 5] to design and implement a *practical* algorithm for computing $Z_p(T) \pmod p$, for all $p < N$ simultaneously. For genus 2 and 3, it is then straightforward to recover the entire zeta function, by applying a baby-step/giant-step algorithm to the group of $\mathbb{F}_p$-rational points on the Jacobian of the curve. For the problem of computing $Z_p(T)$ for all $p < N$ for $N \sim 10^9$, these papers demonstrated a speedup over previous methods by a factor exceeding 300. Consequently it has become possible to numerically study the L-series of genus 2 and 3 hyperelliptic curves over $\mathbb{Q}$ in much greater detail than was previously possible.

However, for $g \geq 4$, knowledge of $Z_p(T) \pmod p$ is insufficient to deduce the entire zeta function efficiently. In this abstract we sketch a proof of the following:

Theorem. *Let $F(x)$ and X_p be as above. There is a deterministic algorithm that computes $Z_p(T)$ for all $p < N$ in time $g^{4+\epsilon} N (\log N)^{3+\epsilon}$ (for large enough N as above).*

The algorithm is considerably simpler than that of [2], and crucially, the exponent of g is reduced from 8 to 4. The author expects that this new algorithm will bring curves of moderate genus, say $4 \leq g \leq 10$, into the range of practical computation.

It is possible to obtain the new complexity bound using the same Monsky–Washnitzer cohomology framework deployed in [2] (which was inherited from Kedlaya's algorithm). However, we take this opportunity to instead use a "trace formula" introduced by the author in [3]. The new bound is thus obtained without the use of any cohomology. The main source of the speedup relative to [2] is the replacement of the rather artificial "reduction towards zero" device from [2] by the simpler "generic prime" trick introduced in [3].

2. The algorithm

We give only a sketch, leaving out many technical details, especially management of the p-adic precision loss caused by divisions by p. We also give no details of the complexity analysis.

Let $X'_p = X_p - \{x = 0, \infty\}$, i.e., the original curve minus the points on the y-axis or at infinity. Below we will give a formula that counts the number of $\mathbb{F}_{p^r}$-rational points on X'_p, modulo p^λ, for arbitrary $\lambda \geq 1$ and $r \geq 1$, provided that $p > 2\lambda$. To determine $Z_p(T)$ it suffices to evaluate this formula for $r = 1, \ldots, g$ and for $\lambda = O(g)$, and then to make trivial corrections for the deleted points.

Let $\alpha_\lambda(t) = \sum_{s=0}^{2\lambda-1} \alpha_{\lambda,s} t^s \in \mathbb{Q}[t]$ be the polynomial defined by the conditions $\alpha_\lambda = 1 \bmod (1-t)^\lambda$ and $\alpha_\lambda = -1 \bmod (1+t)^\lambda$. One checks that $\alpha_\lambda(t)$ is odd and has coefficients in $\mathbb{Z}[\frac{1}{2}]$. Let $G = F^{(p-1)/2} \in \mathbb{Z}[x]$ and for $s \geq 1$ let A_s be the square matrix defined by $(A_s)_{i,j} = (G^s)_{pi-j}$, i.e., the coefficient of x^{pi-j} in G^s, for $0 \leq i, j \leq \lfloor \frac{1}{2} s \deg F \rfloor$. Then our counting formula is

$$|X'_p(\mathbb{F}_{p^r})| = (p^r - 1)\left[1 + \sum_{s=1}^{2\lambda-1} \alpha_{\lambda,s} \operatorname{tr}((A_s)^r)\right] \pmod{p^\lambda}.$$

The proof is elementary, and follows the same lines as the proof of an analogous point-counting formula for general hypersurfaces given in [3].

Our main task is thus to compute the matrices $A_1, A_3, \ldots, A_{2\lambda-1}$, modulo p^λ, for all p simultaneously. In other words, we must compute the coefficients of $G^s = F^{s(p-1)/2}$ in the vicinity of x^{ip}, for small values of s and i. Here "small" means depending only on g, and not on p. For technical reasons our algorithm will actually compute the coefficients of $F^{(sp-1)/2}$; it is then straightforward to solve for the desired coefficients of $F^{s(p-1)/2}$.

Let $d = \deg F$. For $m, k \geq 0$ let V_k^m be the row vector

$$[F^m_{k-d+1}, \ldots, F^m_{k-1}, F^m_k] \in \mathbb{Z}^d,$$

consisting of d consecutive coefficients of F^m. From the relations $F^{m+1} = F \cdot F^m$ and $(F^{m+1})' = (m+1)F' \cdot F^m$ we may deduce (see for example [5]) the recurrence relation $V_k^m = (2kF_0)^{-1} V_{k-1}^m M_k^m$ where M_k^m is the matrix

$$\begin{bmatrix} 0 & 0 & & 0 & (d(2m+2)-2k)F_d \\ 2kF_0 & 0 & \ldots & 0 & ((d-1)(2m+2)-2k)F_{d-1} \\ 0 & 2kF_0 & & 0 & \vdots \\ & & \ddots & & \\ 0 & 0 & \ldots & 2kF_0 & ((2m+2)-2k)F_1 \end{bmatrix}.$$

(We tacitly assume that F has nonzero constant term. If the constant term is zero the algorithm becomes slightly simpler.)

Since we only need bunches of coefficients of $F^{(sp-1)/2}$ spaced out by intervals of p, the central issue is to compute products of the type

$$M_{ip-p+1}^{(sp-1)/2} \cdots M_{ip-1}^{(sp-1)/2} M_{ip}^{(sp-1)/2} \pmod{p^\lambda},$$

which allow us to skip p steps of the recurrence at a time. These products depend on p in three ways: (1) the number of terms in the product, (2) the modulus p^λ, and (3) the matrix entries themselves, via the dependence on the superscripts $m = (sp-1)/2$ and the subscripts $k = ip - j$.

To work around these difficulties, let us introduce indeterminates T and U and consider the matrices $Q_j = M_{U-j}^{(T-1)/2}$ for $j \geq 0$, i.e., each Q_j is obtained by substituting $(T-1)/2$ and $U - j$ for m and k in the formula for M_k^m, interpreting the result as a $d \times d$ matrix over the ring $\mathbb{Z}[U,T]/((U,T)^\lambda)$. Note that Q_j is independent of p, but if we evaluate it at $T = sp$ and $U = ip$, we obtain simply $M_{ip-j}^{(sp-1)/2} \pmod{p^\lambda}$. Thus it suffices to compute $Q_{p-1} \cdots Q_1 Q_0 \pmod{p^\lambda}$, as a matrix over $(\mathbb{Z}/p^\lambda\mathbb{Z})[U,T]/((U,T)^\lambda)$, simultaneously for all odd primes p up to the prescribed bound N. This can be achieved efficiently via a suitable generalisation of the *accumulating remainder tree* from [2]; instead of matrices of integers, we now work with matrices of truncated power series in T and U. We finally make suitable substitutions for T and U, as above, to obtained the desired products.

References

[1] L.M. Adleman and M.D. Huang, *Counting points on curves and abelian varieties over finite fields*, J. Symbolic Comput. **32** (2001), no. 3, 171–189.

[2] D. Harvey, *Counting points on hyperelliptic curves in average polynomial time*, Ann. of Math. (2) **179** (2014), no. 2, 783–803.

[3] ———, *Computing zeta functions of arithmetic schemes*, preprint `http://arxiv.org/pdf/1402.3439.pdf`, 2014.

[4] D. Harvey and A.V. Sutherland, *Computing Hasse-Witt matrices of hyperelliptic curves in average polynomial time*, LMS J. Comput. Math. **17** (2014), no. suppl. A, 257–273.

[5] D. Harvey and A.V. Sutherland, *Computing Hasse-Witt matrices of hyperelliptic curves in average polynomial time, II*, to appear in *Frobenius Distributions*, Contemporary Mathematics, AMS, preprint `http://arxiv.org/abs/1410.5222`.

[6] K.S. Kedlaya, *Counting points on hyperelliptic curves using Monsky-Washnitzer cohomology*, J. Ramanujan Math. Soc. **16** (2001), no. 4, 323–338.

[7] J. Pila, *Frobenius maps of abelian varieties and finding roots of unity in finite fields*, Math. Comp. **55** (1990), no. 192, 745–763.

[8] R. Schoof, *Elliptic curves over finite fields and the computation of square roots mod p*, Math. Comp. **44** (1985), no. 170, 483–494.

Chabauty without the Mordell-Weil group

Michael Stoll

Let C be a smooth projective and geometrically irreducible curve over $\mathbb{Q}$ of genus g at least 2. Then C has finitely many rational points, and it is an interesting problem to determine this finite set explicitly.

Assume that we already know some rational point P_0 on C, so that we know that the set in question is non-empty. The usual procedure for attacking this problem uses the Jacobian variety J of C, which is an abelian variety over $\mathbb{Q}$ of dimension g. Taking P_0 as base-point, we obtain an embedding i of C into J, defined over $\mathbb{Q}$. The task can then be reformulated as 'determine the intersection of $i(C)$ with the group of rational points on J'. The latter group $J(\mathbb{Q})$ is the *Mordell-Weil group*; it is known to be finitely generated. To proceed, we need explicit generators of a subgroup of finite index. We compute a suitable *Selmer group* $\operatorname{Sel}_p J$ of J for some prime p; this is a group that contains an isomorphic image of the quotient $J(\mathbb{Q})/pJ(\mathbb{Q})$ and so its size allows us to deduce an upper bound for the free abelian rank of $J(\mathbb{Q})$. We then have to find the corresponding number of independent points in $J(\mathbb{Q})$. At this point, the procedure is likely to fail when g is not very small and the rank bound is larger than the lower bound obtained from known rational points on C. When this step is successful and the rank is strictly less than g, then a combination of Chabauty's method and the Mordell-Weil sieve is usually successful.

In this talk, we presented a method that avoids the problematic step by working with the Selmer group as a proxy for the Mordell-Weil group. The method may fail in cases when the standard approach would work when provided with generators of a finite-index subgroup. However, on heuristic grounds, failure is unlikely when g is not very small, which is exactly the situation when finding the generators tends to be difficult.

The main idea is to use a variant of the method used in [1] to show that 'most' odd degree hyperelliptic curves have the point at infinity as their only rational point. This variant avoids the use of abelian integrals; instead it relies on computing p-division points of points in $J(\mathbb{Q}_p)$. We have worked it out in some detail for odd degree hyperelliptic curves. For details, see the preprint [2]. One application is the following.

Theorem. Let p be an odd prime. If $p \leq 19$ or, assuming GRH, if $p \leq 53$, then the only rational points on

$$C_p \colon 5y^2 = 4x^p + 1$$

are the obvious ones: $\infty, (1,1), (1,-1)$.

By a result of Dahmen and Siksek, this implies that the only coprime integer solutions of the Generalized Fermat Equation

$$x^5 + y^5 = z^p$$

are the trivial ones (with $xyz = 0$) for the range of primes p in the theorem.

References

[1] B. Poonen, M. Stoll, *Most odd degree hyperelliptic curves have only one rational point*, Ann. Math. 180:3, 1137–1166, (2014).

[2] M. Stoll, *Chabauty without the Mordell-Weil group*, Preprint (2015), arXiv:1506.04286 [math.NT]

Quadratic Chabauty over number fields

Jennifer S. Balakrishnan
(joint work with A. Besser and J.S. Müller)

One of the best tools for explicitly finding rational points on higher genus curves is the method of Chabauty-Coleman [3]; for a smooth projective curve $X/\mathbb{Q}$ of genus g whose Jacobian J has Mordell-Weil rank less than or equal to $g-1$, the method produces a finite set of p-adic points on the curve, among which lie the rational points $X(\mathbb{Q})$.

More precisely, fix an odd prime p such that X has good reduction at p, and let $\{\omega_0, \ldots, \omega_{g-1}\}$ denote a basis of regular 1-forms on X. Suppose $X(\mathbb{Q}) \neq \emptyset$ and fix $b \in X(\mathbb{Q})$. Define locally analytic functions $f_i : X(\bar{\mathbb{Q}}_p) \to \bar{\mathbb{Q}}_p$ by

$$f_i(z) = \int_b^z \omega_i,$$

and extend them linearly to functionals $f_i : J(\mathbb{Q}) \otimes \mathbb{Q} \to \mathbb{Q}_p$.

The method of Chabauty-Coleman can be interpreted as follows: if the Mordell-Weil rank of $J(\mathbb{Q})$ is less than or equal to $g-1$, then one can construct a function given by a $\mathbb{Q}_p$-linear combination of the f_i on $J(\mathbb{Q}_p)$ that vanishes on $J(\mathbb{Q})$. By restricting this function to $X(\mathbb{Q}_p)$, one can approximate the points $X(\mathbb{Q})$. More generally, for a curve X over a degree d number field $K/\mathbb{Q}$, Siksek [4] has given a Chabauty-Coleman method which is likely to work when the Mordell-Weil rank of $J(K)$ is less than or equal to $d(g-1)$.

In the spirit of the Chabauty-Coleman method, in previous work with Besser and Müller [1], we gave a "quadratic" Chabauty method for those curves $X/\mathbb{Q}$ with Mordell-Weil rank equal to g and used this to find integral points on affine models of hyperelliptic curves. Fix an affine model of X and suppose p is a prime of good, ordinary reduction. When the f_i above are linearly independent, quadratic Chabauty makes use of a natural basis of the space of $\mathbb{Q}_p$-valued quadratic forms on $J(\mathbb{Q})$, given by

$$\{f_i \cdot f_j\}_{0 \leq i \leq j \leq g-1},$$

together with the observation that the global p-adic height $h(z)$ on $J(\mathbb{Q})$ is also a quadratic form. This allows us to rewrite $h(z)$ as a $\mathbb{Q}_p$-linear combination of the natural basis of quadratic forms: $h(z) = \sum \alpha_{ij} f_i(z) f_j(z)$.

Moreover, this global p-adic height h admits a decomposition into a sum of local heights h_v: a finite sum of local heights at primes away from p, and a distinguished local height h_p at p, which we know to be a Coleman function by the work of Coleman-Gross [2]. In [1], we proved that the local height at p has a natural interpretation as a sum of double Coleman integrals $D(z)$; we also showed that the local heights away from p take on an effectively computable, finite set of values T on integral points.

Putting it all together, we obtain a p-adic power series from the difference

$$h(z) - h_p(z) = \sum_{i \leq j \leq g-1} \alpha_{ij} f_i(z) f_j(z) - D(z).$$

Since this is just the sum of local heights away from p, we set this power series equal to each element of T and find the set of p-adic points on X satisfying this relationship, among which lie the integral points on X.

This talk presents work in progress extending this quadratic Chabauty method to genus g curves X over degree d number fields $K/\mathbb{Q}$, using a collection of independent p-adic height functions. Indeed, up to nontrivial scalar multiple, the set of independent global p-adic heights on J/K is known to be in one-to-one correspondence with a certain set of $\mathbb{Z}_p$-extensions of K.

By re-writing each of these global p-adic height functions in terms of a natural basis of quadratic forms and computing the decomposition of each global p-adic height into a sum of local heights, we obtain a multivariate system of p-adic power series taking on a finite number of values. Among those p-adic points satisfying the system, we hope to find the points in $X(K)$ defined over $\mathcal{O}_K$.

Generically, this approach works for those curves satisfying the following condition on ranks:

$$\operatorname{rank}(J(K)) + \operatorname{rank}(\mathcal{O}_K^\times) \leq dg.$$

We give two explicit examples where we have carried out this process. Taking K to be $\mathbb{Q}(\sqrt{-3})$, we can reconstruct those points in $X(K)$ defined over $\mathcal{O}_K$ in examples where (1) $X/\mathbb{Q}$ is an elliptic curve with $\operatorname{rank} X(\mathbb{Q}) = 1$ and $\operatorname{rank} X(K) = 2$ and (2) $X/\mathbb{Q}$ is a genus 2 curve with $\operatorname{rank} J(\mathbb{Q}) = 2$ and $\operatorname{rank} J(K) = 4$.

References

[1] J.S. Balakrishnan, A. Besser, and J.S. Müller, *Quadratic Chabauty: p-adic height pairings and integral points on hyperelliptic curves*, J. Reine Angew. Math., to appear.

[2] R.F. Coleman and B.H. Gross, *p-adic heights on curves*, Algebraic Number Theory – in honor of K. Iwasawa, Advanced Studies in Pure Mathematics, **17** (1989), 73–81.

[3] R.F. Coleman, *Effective Chabauty*, Duke Math. J. **52** (1985), no. 3, 765–770.

[4] S. Siksek, *Explicit Chabauty over number fields*, Algebra Number Theory **7** (2013), no. 4, 765–793.

Correct one sided estimates for Manin's conjecture for all smooth cubic surfaces of arithmetic Picard rank greater than three.

Efthymios Sofos

Manin's conjecture [6] postulates that $\mathbb{Q}$–rational points of bounded height on Fano varieties should follow a precise asymptotic distribution. More specifically, let V be a Fano variety defined over a number field K, let H be a height function which is relative to the anticanonical divisor and assume that $V(K)$ is Zariski dense in V. Then there exists a non-empty Zariski open subset $U \subset V$ such that the counting function of K-rational points of bounded height, defined by

$$N_{U,H}(B) := \#\{x \in U(K) : H(x) \leq B\}$$

for $B \geq 1$, satisfies

$$N_{U,H}(B) \sim cB(\log B)^{\rho-1},$$

as $B \to \infty$. Here $\rho = \rho(V, K)$ is the rank of the Picard group of V over K and $c = c(V, H, K)$ is a positive constant that was later studied by Peyre [8].

When the dimension of V is large compared to its degree the conjecture has been established using the Hardy–Littlewood circle method, however the conjecture is far from settled in low dimension and in recent years the dimension 2 case has been an intensive topic of research. Fano varieties of dimension 2 are called del Pezzo surfaces and are classified according to their degree which is an integer $1 \leq d \leq 9$. Here U is taken as the compliment in V of the finitely many exceptional curves. The conjecture is known when $d \geq 6$ [1] while in the case $d = 5$ it is only proved for split surfaces and $K = \mathbb{Q}$ [2]. Regarding the case $d = 4$ the conjecture has recently been settled for a single smooth surface and only in the case $K = \mathbb{Q}$ [3].

Regarding the cases $d = 1, 2, 3$ there has been no example of a smooth del Pezzo surface for which the conjecture has been established. When $d = 3$, i.e. the case of smooth cubic surfaces, there has been a long list of partial results towards the conjecture, of which we only mention the most optimal: Regarding upper bounds, Salberger [10] has proved, using Heath–Brown's determinant method, that for all smooth cubic surfaces, for $K = \mathbb{Q}$ and all $\epsilon > 0$ one has

$$N_{U,H}(B) \ll_\epsilon B^{12/7+\epsilon}$$

while the best exponent regarding upper bounds has been obtained by Heath–Brown [7], who used conic bundles to show that in the case $K = \mathbb{Q}$ one has

$$N_{U,H}(B) \ll_{\epsilon,V} B^{4/3+\epsilon}$$

for all smooth cubic surfaces which contain 3 rational coplanar lines. This result has been recently extended to all number fields K in [4]. Regarding lower bounds there has only been the work of Swinnerton–Dyer and Slater [11] where they proved the correct lower bound

$$N_{U,H}(B) \gg_V B(\log B)^{\rho-1},$$

for $K = \mathbb{Q}$ and all smooth cubic surfaces with 2 rational lines ℓ_1, ℓ_2 which do not meet. The proof uses the parametrisation of the cubic surface obtained by the fact that it is birational to $\ell_1 \times \ell_2$ over the ground field. This result however does not cover the Fermat cubic surface which has arithmetic Picard rank 4, since its only skew lines are defined over $\mathbb{Q}(\sqrt{-3})$. Furthermore for each $i = 1, \ldots, 6$, the generic smooth cubic surface of arithmetic Picard rank $\rho = i$ does not contain two skew lines defined over the ground field.

The object of this talk is to provide a report on the following result that appeared in the author's PhD thesis.

Theorem. *Let V be a smooth cubic surface defined over $\mathbb{Q}$ and assume that it has arithmetic Picard rank $\rho > 3$. Then the correct lower bound according to Manin's conjecture holds, namely we have*

$$N_{U,H}(B) \gg_V B(\log B)^{\rho-1},$$

as $B \to \infty$.

Any surface as above must contain a rational line, as seen for example in Table 2 of [9, Appendix] and therefore V is endowed with a conic bundle structure over $\mathbb{Q}$. Counting points on the fibers of small height and using Theorem 1 of the author's work [12] which proves Manin's conjecture for the fibers with a uniform error term, one can reduce the problem of counting points on the surface to one of estimating the average of the Peyre constants of the fibers. A significant obstacle here is that the generic fiber will have no rational point and thus almost all Peyre constants will vanish. We overcome this issue by using information about the conic bundle structure to construct detector functions that can pick the fibers which have a rational point. One can then reduce the problem to one of estimating asymptotically a sum of the form

$$\sum_{\substack{n,m\in\mathbb{Z}^2\\|n|,|m|\leq x}}\prod_{i=1}^{s}\left(\sum_{\substack{d_i\in\mathbb{N}\\d_i|f_i(n,m)}}1\right)\prod_{j=1}^{r}\left(\sum_{\substack{d_j\in\mathbb{N}\\d_j|f_j(n,m)}}\left(\frac{g_j(n,m)}{d_j}\right)\right),$$

where $\left(\frac{\cdot}{d}\right)$ is the quadratic Jacobi symbol and the irreducible binary integer forms f_i are associated to the split fibers of the conic bundle and similarly the pairs of binary integer forms (f_i, g_i) are associated to the non–split fibers. The final step of the proof is to evaluate the previous sum using the approach initially introduced in [5] for evaluating the average of the number of representations as a sum of two squares of the integer values assumed by an irreducible integer form of degree at most 4.

References

[1] V.V. Batyrev, Y. Tschinkel, *Manin's conjecture for toric varieties*, J. Alg. Geom. **7** (1998), 15–53.

[2] R. de la Bretèche, *Nombre de points de hauteur bornè sur les surfaces de del Pezzo de degrè 5*, Duke Math. J. **13** (2002), 421–464.

[3] R. de la Bretèche, T. Browning, *Manin's conjecture for quartic del Pezzo surfaces with a conic fibration*, Duke Math. J. **160** (2011), 1–69.

[4] T. Browning, M. Swarbrick Jones, *Counting rational points on del Pezzo surfaces with a conic bundle structure*, Acta Arithmetica **163** (2014), 271–298.

[5] S. Daniel, *On the divisor–sum problem for binary forms*, J. reine angew. Math. **507** (1999), 107–129.

[6] J. Franke, Y. I. Manin, Y. Tschinkel, *Rational points of bounded height on Fano varieties*, Inventiones Mathematicae **95** (1989), 421–435.

[7] D. R. Heath-Brown, *The density of rational points on cubic surfaces*, Acta Arithmetica **1** (1997), 17–30.

[8] E. Peyre, *Hauteurs et mesures de Tamagawa sur les varièt̀es de Fano*, Duke Math. J. **79** (1995), 101–218.

[9] J. Jahnel, *Brauer groups, Tamagawa measures, and rational points on algebraic varieties*, Mathematical Surveys and Monographs **198** AMS, Providence (2014).

[10] P. Salberger, *Counting rational points on projective varieties*, In preparation, (2014).

[11] J.B. Slater, P. Swinnerton-Dyer, *Counting points on cubic surfaces. I*, Astèrisque **251** (1998), 1–12.

[12] E. Sofos, *Uniformly counting rational points on conics*, Acta Arithmetica **166** (2014), 1–13.

Reporter: Efthymios Sofos

Participants

Dr. Jennifer S. Balakrishnan
Mathematical Institute
Oxford University
Andrew Wiles Building
Woodstock Road
Oxford OX2 6GG
UNITED KINGDOM

Alex Bartel
Mathematics Institute
University of Warwick
Zeeman Building
Coventry CV4 7AL
UNITED KINGDOM

Prof. Dr. Karim Belabas
Institut de Mathématiques
Université de Bordeaux
351, cours de la Liberation
33405 Talence Cedex
FRANCE

Prof. Dr. Michael A. Bennett
Department of Mathematics
University of British Columbia
121-1984 Mathematics Road
Vancouver BC V6T 1Z2
CANADA

Prof. Dr. Daniel J. Bernstein
Department of Computer Science
University of Illinois at Chicago
M/C 249, 322 SEO
851 S. Morgan Street
Chicago IL 60607-7045
UNITED STATES

Prof. Dr. Frits Beukers
Mathematisch Instituut
Universiteit Utrecht
Budapestlaan 6
P. O. Box 80.010
3508 TA Utrecht
NETHERLANDS

Prof. Dr. Manjul Bhargava
Department of Mathematics
Princeton University
Fine Hall
Washington Road
Princeton, NJ 08544
UNITED STATES

Dr. Andrew Booker
Department of Mathematics
University of Bristol
University Walk
Bristol BS8 1TW
UNITED KINGDOM

Prof. Dr. Nils Bruin
Dept. of Mathematics and Statistics
Simon Fraser University
Burnaby, B.C. V5A 1S6
CANADA

Prof. Dr. Frank Calegari
Department of Mathematics
Northwestern University
Lunt Hall
2033 Sheridan Road
Evanston, IL 60208-2730
UNITED STATES

Prof. Dr. Henri Cohen
Institut de Mathématiques
Université de Bordeaux
351, cours de la Liberation
33405 Talence Cedex
FRANCE

Prof. Dr. John E. Cremona
Mathematics Institute
University of Warwick
Gibbet Hill Road
Coventry CV4 7AL
UNITED KINGDOM

Prof. Dr. Christophe Delaunay
Faculté des Sciences et Techniques
Laboratoire Mathématiques de Besancon
Université de Franche-Comte
16, route de Gray
25030 Besancon Cedex
FRANCE

Dr. Bart de Smit
Mathematisch Instituut
Universiteit Leiden
Postbus 9512
2300 RA Leiden
NETHERLANDS

Prof. Dr. Tim Dokchitser
Department of Mathematics
University of Bristol
University Walk
Bristol BS8 1TW
UNITED KINGDOM

Prof. Dr. Bas Edixhoven
Mathematisch Instituut
Universiteit Leiden
Postbus 9512
2300 RA Leiden
NETHERLANDS

Dr. Tom A. Fisher
Centre for Mathematical Sciences
University of Cambridge
Wilberforce Road
Cambridge CB3 0WB
UNITED KINGDOM

Dr. Herbert Gangl
Dept. of Mathematical Sciences
Durham University
Science Laboratories
South Road
Durham DH1 3LE
UNITED KINGDOM

Prof. Dr. Andrew J. Granville
Dept. of Mathematics and Statistics
University of Montreal
CP 6128, succ. Centre Ville
Montreal, QC H3C 3J7
CANADA

Prof. Dr. Benedict H. Gross
Department of Mathematics
Harvard University
Science Center
One Oxford Street
Cambridge MA 02138-2901
UNITED STATES

Prof. Dr. Paul E. Gunnells
Dept. of Mathematics & Statistics
University of Massachusetts
710 North Pleasant Street
Amherst, MA 01003-9305
UNITED STATES

Dr. David Harvey
School of Mathematics & Statistics
The University of New South Wales
Sydney NSW 2052
AUSTRALIA

Prof. Dr. Wei Ho
Department of Mathematics
University of Michigan
East Hall
530 Church Street
Ann Arbor, MI 48109-1109
UNITED STATES

Prof. Dr. Kiran S. Kedlaya
Department of Mathematics
University of California, San Diego
9500 Gilman Drive
La Jolla, CA 92093-0112
UNITED STATES

Prof. Dr. Jürgen Klüners
Institut für Mathematik
Universität Paderborn
Warburger Str. 100
33098 Paderborn
GERMANY

Prof. Dr. Hendrik W. Lenstra
Mathematisch Instituut
Universiteit Leiden
Postbus 9512
2300 RA Leiden
NETHERLANDS

Dr. Nicolas Mascot
Mathematics Institute
University of Warwick
Gibbet Hill Road
Coventry CV4 7AL
UNITED KINGDOM

Dr. Anton Mellit
International Centre for Theoretical
Physics (ICTP)
LB Room 126
Strada Costiera, 11
34100 Trieste
ITALY

Prof. Dr. Jean-Francois Mestre
U. F. R. de Mathématiques
Université Paris 7
Case 7012
175, rue de Chevaleret
75013 Paris Cedex
FRANCE

Prof. Dr. Hartmut Monien
Physikalisches Institut
Universität Bonn
Nußallee 12
53115 Bonn
GERMANY

Prof. Dr. Ariel Martin Pacetti
Depto. de Matematica - FCEN
Universidad de Buenos Aires
Ciudad Universitaria
Pabellon 1
Buenos Aires C 1428 EGA
ARGENTINA

Dr. Aurel Page
Mathematics Institute
University of Warwick
Gibbet Hill Road
Coventry CV4 7AL
UNITED KINGDOM

Dr. Jennifer Park
Department of Mathematics
McGill University
845 Sherbrooke Street West
Montreal, QC H3A 0G4
CANADA

Prof. Dr. Bjorn Poonen
Department of Mathematics
Massachusetts Institute of Technology
77 Massachusetts Ave.
Cambridge, MA 02139-4307
UNITED STATES

Prof. Dr. David Roberts
Division of Science and Mathematics
University of Minnesota - Morris
Morris, MN 56267
UNITED STATES

Prof. Dr. Fernando Rodriguez-Villegas
Mathematics Section
The Abdus Salam International Centre
for Theoretical Physics (ICTP)
Strada Costiera, 11
34151 Trieste
ITALY

Prof. Dr. René Schoof
Dipartimento di Matematica
Universita degli Studi di Roma II
Tor Vergata
Via della Ricerca Scientifica
00133 Roma
ITALY

Prof. Dr. Jean-Pierre Serre
6, Avenue de Montespan
75116 Paris
FRANCE

Prof. Dr. Samir Siksek
Department of Mathematics
University of Warwick
Coventry CV4 7AL
UNITED KINGDOM

Dr. Efthymios Sofos
Mathematical Institute
Leiden University
Snellius Bldg., office 225
Niels Bohrweg 1
2333 CA Leiden
NETHERLANDS

Prof. Dr. Peter Stevenhagen
Mathematisch Instituut
Universiteit Leiden
Postbus 9512
2300 RA Leiden
NETHERLANDS

Prof. Dr. Michael Stoll
Mathematisches Institut
Universität Bayreuth
95440 Bayreuth
GERMANY

Dr. Andrew Sutherland
Department of Mathematics
Massachusetts Institute of Technology
77 Massachusetts Ave.
Cambridge, MA 02139-4307
UNITED STATES

Dr. Ha Tran
Dept. of Mathematics & Systems
Analysis
Aalto University
School of Science
Otakaari 1
02150 Espoo 15
FINLAND

Prof. Dr. Douglas Ulmer
School of Mathematics
Georgia Institute of Technology
686 Cherry Street
Atlanta, GA 30332-0160
UNITED STATES

Prof. Dr. Anthony Varilly-Alvarado
Department of Mathematics
Rice University; MS 136
P.O. Box 1892
Houston, TX 77005-1892
UNITED STATES

Dr. Masha Vlasenko
School of Mathematical Sciences
University College Dublin
G 12 Science Centre North, Belfield
Dublin 4
IRELAND

Dr. John Voight
Dept. of Mathematics & Computer Science
Dartmouth College
6188 Kemeny Hall
Hanover, NH 03755-3551
UNITED STATES

Xiaoheng Jerry Wang
Department of Mathematics
Princeton University
Fine Hall
Washington Road
Princeton, NJ 08544-1000
UNITED STATES

Dr. Mark J. Watkins
MAGMA Computer Algebra Group
School of Mathematics & Statistics
The University of Sydney
Carslaw Building (F07)
Sydney NSW 2006
AUSTRALIA

Prof. Dr. Don B. Zagier
Max-Planck-Institut für Mathematik
Vivatsgasse 7
53111 Bonn
GERMANY

Dr. David Zywina
Department of Mathematics
Cornell University
Malott Hall
Ithaca, NY 14853
UNITED STATES