Mathematisches Forschungsinstitut Oberwolfach

Report No. 34/2007

Explicit Methods in Number Theory

Organised by
Henri Cohen, Talence
Hendrik W. Lenstra, Leiden
Don B. Zagier, Bonn

July 15th – July 21st, 2007

Abstract. These notes contain extended abstracts on the topic of explicit methods in number theory. The range of topics includes asymptotics for field extensions and class numbers, random matrices and L-functions, rational points on curves and higher-dimensional varieties, and aspects of lattice basis reduction.

Mathematics Subject Classification (2000): 11–xx, 12–xx, 13–xx, 14–xx.

Introduction by the Organisers

The workshop *Explicit Methods in Number Theory* was organised by Henri Cohen (Talence), Hendrik W. Lenstra (Leiden), and Don B. Zagier (Bonn), with the assistance of Karim Belabas (Talence), and it took place July 15–21, 2007. Four previous workshops on the topic had been held in 1999, 2001, 2003, and 2005. 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 were three 'mini-series' highlighting important recent developments: one of three hours, by Jordan Ellenberg and Akshay Venkatesh, on asymptotics for field extensions and class numbers; one of two hours by Mark Watkins, on random matrices and L-functions; and one of three hours by Noam Elkies, on the construction of elliptic curves of high Mordell–Weil rank.

Some of the other themes were:

- Modular forms
- Rational and integral points on curves and higher-dimensional varieties
- Counting points on varieties over finite fields
- Fast multiplication
- Aspects of lattice basis reduction.

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 51 participants from a variety of backgrounds, including a large number of younger researchers. There were 32 talks of various lengths, and ample time was allotted to informal collaboration.

Workshop: Explicit Methods in Number Theory

Table of Contents

Abstracts

Asymptotics for field extensions and class numbers and topology of Hurwitz spaces, I, II, III

Jordan S. Ellenberg and Akshay Venkatesh

We are currently thinking about some long-standing problems about distribution of discriminants of number fields and asymptotics of p-parts of class numbers; more specifically, we are interested in the ways that the geometry arising from the function-field analogues of these questions can give insights into phenomena occuring over number fields.

Here are two sample questions:

Question 1: Let $r_p(D)$ be the p-rank of the class group of $\mathbb{Q}(\sqrt{-D})$. What is the average value of $p^{r_p(D)}$ as D ranges between 0 and X? What is the probability distribution on $r_p(D)$? What are upper bounds on $r_p(D)$ in terms of D?

Question 2: Let D be a squarefree integer and let $n(D)$ be the number of S_5-extensions of discriminant D. What is the average value of $n(D)$ as D ranges between $-X$ and X? What is the probability distribution on $n(D)$? What are upper bounds for $n(D)$ in terms of D?

Some remarks:

- The second part of Question 1 is of course the subject of the Cohen-Lenstra heuristics.
- The third part of Question 1 (upper bounds on $r_p(D)$) has been the subject of quite a bit of recent interest. A folklore conjecture holds that $p^{r_p(D)} \ll_{p,\epsilon} D^{\epsilon}$. But at present one knows how to beat the trivial bound $p^{r_p(D)} \ll D^{1/2+\epsilon}$ only by a small power of D, and even then only for $p = 3$ without assuming a Riemann hypothesis.

The two questions are really of a similar flavor, in the following sense: $p^{r_p(D)}$ can be thought of as measuring the number of degree-p extensions of $\mathbb{Q}$ with dihedral Galois group D_p and discriminant $D^{(p-1)/2}$. So in both cases we are studying the number of field extensions of $\mathbb{Q}$ with given Galois group and discriminant. Thus, the "average value" part of the questions fall under the purview of Malle's conjecture, which we recall here: if $G \subset S_n$, and $N_{G,n}(X)$ is the number of degree-n extensions of a number field K with Galois group G and discriminant at most X, then Malle conjectures that

$$N_{G,n}(X) \sim c(G,K)X^{a(G)}(\log X)^{b(G,K)-1}$$

where a, b are explicit constants. Bhargava has conjectured values for $c(G,\mathbb{Q})$ when $G = S_n$, which agree with known values for $n \leq 5$. The value of $b(G,K)$ originally conjectured by Malle was shown to be incorrect in some cases by Klüners; in recent work, Türkelli has proposed a modified definition which seems a reasonable substitute and which admits no known counterexamples.

A main theme of our recent work is to study the above questions in the case where the base field K is the function field of a curve $C/\mathbb{F}_q$. In that case, one has that $N_{G,n}(X)$ counts covers of the curve C with fixed Galois group and discriminant bounded by X. Such covers are parametrized by a moduli space $H_{G,n,X}$ called a *Hurwitz space*. (For example, double covers of $\mathbb{P}^1$ with discriminant at most q^{2g+2} are parametrized by the moduli space of hyperelliptic curves of genus at most g, a particularly tractable example.)

In this setting, one has the great advantage that one can use the algebraic geometry of the Hurwitz space $H_{G,n,X}$ in order to estimate the cardinality of $H_{G,n,X}(\mathbb{F}_q)$. In particular, by the Lefschetz trace formula one can control this number of points by controlling the cohomology of $H_{G,n,X}$. It turns out that there is a very natural guess to make: namely, that these Hurwitz spaces (more precisely, variants of these which parametrize things like "covers with squarefree discriminant") have the same cohomology as affine space in a large range of dimensions. In particular, Hurwitz spaces of dimension d ought to have very close to q^d points. The key point is that, by comparison of etale and singular cohomology, the necessary vanishing of cohomology is a *purely topological* assertion about the complex points of $H_{G,n,X}$, on which the apparatus of topology and complex algebraic geometry can in principle be brought to bear.

This description has now strayed a bit from "explicit methods," so let us remark on some computational problems which will help to clarify the plausibility of the "master guess" above.

- The conjectures of Malle and of Cohen-Lenstra have been subjected to quite extensive numerical checking over number fields; over function fields, however, much less experimentation has been done, even in the case of S_3-extensions (equivalently, 3-ranks of class groups of quadratic fields) where a very fast algorithm due to Belabas is available in the case $K = \mathbb{Q}$. Explicit computation of $N_{G,n}(X)$ where K is a function field should give very persuasive evidence that the cohomology of various Hurwitz spaces are behaving as we expect (or otherwise!)
- The master guess also implies statements of a "non-abelian Cohen-Lenstra" type over function fields. For instance, it suggests that the function $n(D)$ above (counting S_5-extensions of squarefree discriminant D) obeys a Poisson distribution with mean 1. Can this be investigated experimentally? What about the analogous question over $\mathbb{Q}$ (where the expected mean is $(13/120)\zeta(2)^{-1}$?) (Remark: we are indebted to the recent work of Dunfield and Thurston for alerting us to the fact that the Poisson distribution should arise here – their work concerns, not finite covers of a random number field, but finite covers of a random 3-manifold – but the underlying topological issues turn out to have a great deal in common.)

Asymptotics of class numbers for fundamental discriminants

Nicole Raulf[1]

Let $\mathcal{D} := \{d \in \mathbb{N} : \ d \equiv 0, 1\,(4),\, d \neq \square\}$ and $\mathcal{D}_F := \{d \in \mathcal{D} : \ d \text{ a fundamental discriminant}\}$. For every $d \in \mathcal{D}$ we denote the class number of primitive binary quadratic forms with coefficients in $\mathbb{Z}$ and discriminant d by h_d. Furthermore, ϵ_d is the fundamental solution of Pell's equation $t^2 - du^2 = 4$. Class numbers and their behaviour have been of interest for a long time as can be seen from the works of Gauß, Siegel, Shintani, Datskovsky and other mathematicians. Siegel [Sie] e. g. proved that

$$\sum_{d \leq N} h_d \log \epsilon_d = \frac{\pi^2}{18\zeta(3)}\, N^{3/2} + O(N \log N)$$

as $N \to \infty$. Later Shintani [Shi] improved the error term and Datskovsky [Dat] has the corresponding result for fundamental discriminants. But so far it has not been possible to separate h_d from $\log \epsilon_d$ in these formulas. This problem does not exist anymore when we order the terms according to the size of ϵ_d. Using Selberg's trace formula Sarnak [Sar1] showed that

$$\sum_{\substack{d \in \mathcal{D}, \\ \epsilon_d \leq N}} h_d = \mathrm{Li}\big(N^2\big) + O\big(N^{3/2} \log^2 N\big) \tag{1}$$

as $N \to \infty$. Here $\mathrm{Li}(N) := \int_2^N \frac{dt}{\log t}$. In order to determine the asymptotic behaviour of this sum when we only sum over fundamental discriminants we first consider the expressions

$$\sum_{\substack{d \equiv a\,(m), \\ \epsilon_d \leq N}} h_d \log \epsilon_d$$

for $m \in \mathbb{N}$ and $a \in \mathbb{N}_0$, i. e. we restrict ourselves to class numbers whose discriminants belong to the progression $d \equiv a\,(m)$. For the progression $d \equiv 0\,(m)$ the theorem that gives the asymptotics reads as follows:

Theorem 1 ([Rau]). *For $m \in \mathbb{N}$ let $\tau(m) := \sharp\{p \geq 3 : \ p|m\}$.*

1. *If $m \equiv 0\,(2)$ then*

$$\sum_{\substack{d \equiv 0\,(m), \\ \epsilon_d \leq N}} h_d \log \epsilon_d \sim \frac{2^{\tau(m)}}{56m} \prod_{\substack{p \geq 3, \\ p|m}} \left(1 - p^{-3}\right)^{-1} \begin{Bmatrix} 37, & 2||m, \\ 74, & 4||m, \\ 88, & 8||m, \\ 12^2, & 16||m, \\ 2^8, & 32|m. \end{Bmatrix} \times N^2, \ N \to \infty.$$

[1]Research supported by a fellowship within the PostDoc-Programme of the German Academic Exchange Service (DAAD).

2. *If* $m \equiv 1\,(2)$ *then*

$$\sum_{\substack{d\equiv 0\,(m),\\ \epsilon_d \le N}} h_d \log \epsilon_d \sim \frac{2^{\tau(m)-1}}{m} \prod_{\substack{p\ge 3,\\ p\mid m}} \left(1-p^{-3}\right)^{-1} N^2,\ N\to\infty.$$

For similar formulas for the progressions $d \equiv a \bmod m$, $m \in \mathbb{N}$, $a \in \mathbb{N}_0$, see [Rau]. Moreover, by partial summation the regulators in these formulas can be removed and for $m = 1$ we recover the leading term of (1). With the help of the formulas for class numbers in progressions we finally deduce

Theorem 2 ([Rau])**.** *We have the following asymptotic behaviour:*

$$\sum_{\substack{d\in\mathcal{D}_F,\\ \epsilon_d \le N}} h_d \sim \frac{25\zeta(3)}{16} \prod_{p\ge 2} \left(1-2p^{-2}-p^{-3}\right)\mathrm{Li}(N^2) \quad as \quad N\to\infty.$$

In order to prove Theorem 1 it suffices to understand the behaviour of the sums

$$\sum_{\substack{2<t\le N,\, d(t,u):=\\ (t^2-4)/u^2\in\mathcal{D}_*}} \frac{h_{d(t,u)} \log \epsilon_{d(t,u)}}{\sqrt{d(t,u)}} \tag{2}$$

for $u \in \mathbb{N}$ fixed and "small". Here $\mathcal{D}_* = \{d \in \mathcal{D} :\ d \equiv 0\,(m),\, d \equiv 0\,(4)\}$, $\{d \in \mathcal{D} :\ d \equiv 0\,(m),\, d \equiv 1\,(8)\}$ or $\{d \in \mathcal{D} :\ d \equiv 0\,(m),\, d \equiv 5\,(8)\}$. For determining the asymptotics of (2) one can use the class number formula and discuss $\sum_t L(1, d(t,u))$ where $L(s, d(t,u)) := \sum_{n=1}^{\infty} (d(t,u)/n)\, n^{-s}$ with $(d(t,u)/\cdot)$ being the Kronecker symbol. In different situations this approach for deriving asymptotics of class numbers has been used by Barban [Bar] and by Sarnak [Sar2].

References

[Bar] Barban, M. B.: *The Large Sieve Method And Its Applications in The Theory Of Numbers,* Russian Mathematical Surveys **21** (1966), 49–103.

[Dat] Datskovsky, B. A: *A mean-value theorem for class numbers of quadratic extensions,* A tribute to Emil Grosswald: number theory and related analysis, 179–242, Contemp. Math., 143, Amer. Math. Soc., Providence, RI, 1993.

[Gau] Gauß, C. F.: *Disquisitiones arithmeticae,* Translated and with a preface by Arthur A. Clarke. Revised by William C. Waterhouse, Cornelius Greither and A. W. Grootendorst and with a preface by Waterhouse. Springer-Verlag, New York, 1986.

[Rau] Raulf, N.: *Asymptotics of Class Numbers for Progressions and of Fundamental Discriminants,* Preprint, submitted.

[Sar1] Sarnak, P.: *Class numbers of indefinite binary quadratic forms,* J. Number Theory **15** (1982), no. 2, 229–247.

[Sar2] Sarnak, P. C.: *Class numbers of indefinite binary quadratic forms, II,* J. Number Theory **21** (1985), 333–346.

[Shi] Shintani, T.: *On zeta-functions associated with the vector space of quadratic forms,* J. Fac. Sci. Univ. Tokyo Sect. 1A Math. **22** (1975), 25–65.

[Sie] Siegel, C. L.: *The average measure of quadratic forms with given determinant and signature,* Ann. of Math. (2) **45** (1944), 667–685.

Probabilistic models for *L*-functions, I, II

Mark Watkins

The zeros of the Riemann zeta function were conjectured by Hilbert and Polya to have a spectral interpretation. Work of Montgomery and computations of Odlyzko gave credence to this, especially as the spacings between zeros were well-modelled statistically by the spacings between eigenvalues of random matrices. The fit here is extremely good — we see this as a manifestation that random matrix theory gives very good models for local statistics of L-functions, at least to first order.

On the other hand, global statistics such as moments (which correspond to the evaluation of the characteristic polynomial of a random matrix at some point on the unit circle) do not have such universal behaviour, and so we must introduce arithmetic information into the model. This was done in a largely *ad hoc* manner for moments of the zeta function on the critical line in the work of Keating and Snaith, following earlier work of Conrey and Ghosh. More recently, the Hybrid Model of Gonek, Hughes, and Keating allows us a more natural derivation: the zeta function is approximated by a truncated Euler product times a Weierstrass product of zeros — this is moderated by a parameter X, which tells us to consider the primes up to X and (essentially) the zeros at distance at most $1/\log X$. These contributions from the primes and zeros are suspected to be independent. The Euler product can be analysed rigourously and gives the same arithmetic factor as guessed by Conrey and Ghosh, while the zeros again require an analogy from random matrix theory; the resulting analysis reproduces the conjecture of Keating and Snaith, but gives stronger evidence that the arithmetic and universal behaviour have been combined in an adequate manner. Our hope in this analogy is bolstered by taking function field analogues, for which we can often obtain rigourous results. The above problem uses unitary matrices to model the situation, as will all questions involving zero-spacing or moments in the t-aspect. However, questions about zeros of low height or moments of special values can yield other symmetries: the most common examples are quadratic Dirichlet characters from which we get symplectic symmetry, and the quadratic twists of a fixed elliptic curve, where we see orthogonal symmetry.

The work of Keating and Snaith establishes a result for moments of characteristic polynomials for any of these symmetry types, and we can thus export this result (possibly using analysis similar to the Hybrid Model, or merely at the level of analogy) to predict the moments of $L(E_d, 1)$ in a family of quadratic twists of even parity. Their result gives the s-th moment as a meromorphic function of s, and thus we can obtain a value distribution, whose behaviour for small values is dominated by the rightmost pole. If we consider d close to D, we get a result like

$$\mathrm{Prob}\big[L(E_d, 1) < t\big] \sim \alpha_E t^{1/2} (\log D)^{3/8} \text{ as } t \to 0,$$

where α_E is the arithmetic factor. Here the exponent of $1/2$ comes from the rightmost pole $s = -1/2$ of the moment generating function, while the $3/8$ exponent on the log is $\binom{-1/2}{2}$ — both of these are particular to orthogonal symmetry. From

the conjecture of Birch and Swinnerton-Dyer, we can then introduce a discretisation process which will allow us to predict the number of even parity twists with $L(E_d, 1) = 0$ (arithmetically, we generically expect such twists to have rank 2). In particular, BSD gives us (essentially) a formula

$$S_d = \frac{L(E_d, 1)T^2}{\prod_p c_p(d) \cdot \Omega_{\mathrm{re}}/\sqrt{d}}$$

where S_d is a nonnegative integer. Thus if $S_d < 1$ we have $S_d = 0$. Plugging in the right side of the above for t gives us that

$$\mathrm{Prob}\big[L(E_d, 1) < t\big] \sim \beta_E \cdot \sqrt{\textstyle\prod_p c_p(d)} \cdot (\log d)^{3/8}/d^{1/4}.$$

For $|d|$ that are prime, we understand $c_p(d)$ and so can just sum over d to get a predicted asymptotic of $c_E D^{3/4}(\log D)^{3/8-1}$ for the number of even prime twists up to D for which $L(E_d, 1)$ vanishes. When considering all twists, we must consider the average behaviour of the Tamagawa product, and this essentially depends upon the 2-torsion of E. We get a prediction of $c_E D^{3/4}(\log D)^{b_E}$, where there are four possible values of b_E. Rubinstein has computed much data (using the Waldspurger correspondence and ternary quadratic forms), and they do not show our guesses to be false. Kowalski has theorems about the function field analogues, but these are mostly upper bounds. Assuming the Parity Conjecture, Rubin and Silverberg can construct $D^{1/2}$ twists of rank ≥ 2 for various E, but this is far from our expectation of above. Another item of interest is a conjecture about counts of vanishing twists when restricting to arithmetic progressions modulo a prime — it is expected that quadratic residuacity is the controlling factor, and the ratio between counts for squares and non-squares should be $\left(\frac{p+1+a_p}{p+1-a_p}\right)^{-1/2}$ where the $-1/2$ is the rightmost pole again. Again the data show no obvious contradiction.

David, Fearnley, and Kislievsky consider fixing an elliptic curve E and twisting by cubic Dirichlet characters, which is related to the behaviour of the curve when base-extending to a C_3 extension. Here the symmetry is unitary, and there is no "parity" as the sign of the functional equation can be anywhere on the unit disc. Copying the above methodology, they get a prediction that the number of cubic characters χ with conductor less than D such that $L(E \otimes \chi, 1) = 0$ should be asymptotically $c_E D^{1/2}(\log D)^{b_E}$ where b_E is $1/4$ or $9/4$, depending on whether E has 3-torsion. Fearnley and Kisilevsky can construct $D^{1/2}$ such twists in some cases, which is quite close to the guess. We could also consider $x^3 + y^3 = mz^3$ (where there is no obvious function field analogue), or the set of elliptic curves (ordered by discriminant), and get similar heuristics. In these cases, the data converge to the asymptotic behaviour too slowly to say much, though we are able to refute the "null hypothesis" that a positive proportion of even parity curves have positive rank.

For quadratic twists of odd parity, we can use complex approximations to Heegner points and a theorem of Gross and Zagier to get data of similar bulk to Rubinstein's data for even parity. However, there is no precise conjecture for the number of odd twists with $L'(E_d, 1) = 0$, and a numerical analysis of the data does not

yield a compelling guess even at the crude level. On the other hand, we can readily compute the ratio of vanishings for squares/non-squares modulo a prime, where here we expect $\left(\frac{p+1+a_p}{p+1-a_p}\right)^{-3/2}$ as the rightmost pole is now at $-3/2$. The data do not dispel this suspicion.

References

[1] Baur Bektemirov, Barry Mazur, William Stein, and Mark Watkins, Average ranks of elliptic curves: tension between data and conjecture. *Bull. Amer. Math. Soc. (N.S.)* **44** (2007), no. 2, 233–254 (electronic).
Available at `http://dx.doi.org/10.1090/S0273-0979-07-01138-X`

[2] J. B. Conrey, J. P. Keating, M. O. Rubinstein, and N. C. Snaith, On the frequency of vanishing of quadratic twists of modular L-functions. *Number theory for the millennium, I* (Urbana, IL, 2000), 301–315, A K Peters, Natick, MA, 2002.

[3] ———, Random matrix theory and the Fourier coefficients of half-integral-weight forms. *Experiment. Math.* **15** (2006), no. 1, 67–82.
Available at `http://www.expmath.org/expmath/volumes/15/15.1/Conrey.pdf`

[4] Chantal David, Jack Fearnley, and Hershy Kisilevsky, On the vanishing of twisted L-functions of elliptic curves. *Experiment. Math.* **13** (2004), no. 2, 185–198.
Available at `http://www.expmath.org/expmath/volumes/13/13.2/David.pdf`

[5] S. M. Gonek, C. P. Hughes, and J. P. Keating, Hybrid Euler-Hadamard product for the Riemann zeta function. *Duke Math. J.* **136** (2007), 507–549.
Preprint from `http://arxiv.org/math.NT/0511182`

[6] Nicholas M. Katz and Peter Sarnak, Zeroes of zeta functions and symmetry. *Bull. Amer. Math. Soc. (N.S.)* **36** (1999), no. 1, 1–26.
Available at `http://dx.doi.org/10.1090/S0273-0979-99-00766-1`

[7] J. P. Keating and N. C. Snaith, Random matrix theory and $\zeta(1/2 + it)$. Random matrix theory and L-functions at $s = 1/2$. *Comm. Math. Phys.* **214** (2000), no. 1, 57–89, 91–110.
Available at `http://dx.doi.org/10.1007/s002200000261`,
`http://dx.doi.org/10.1007/s002200000262`

[8] Karl Rubin and Alice Silverberg, Ranks of elliptic curves. *Bull. Amer. Math. Soc. (N.S.)* **39** (2002), no. 4, 455–474 (electronic).
Available at `http://dx.doi.org/10.1090/S0273-0979-02-00952-7`

[9] M. Watkins, Rank distribution in a family of cubic twists. In: *Ranks of Elliptic Curves and Random Matrix Theory*, edited by J. B. Conrey, D. W. Farmer, F. Mezzadri, and N. C. Snaith, 237–246, London Mathematical Society Lecture Note Series #341, Cambridge University Press, 2007.

[10] M. Watkins, Extra rank for odd parity quadratic twists.
Preprint, `http://www.maths.bris.ac.uk/~mamjw/r3.pdf`

Applications of the Mordell–Weil sieve

Michael Stoll

In this talk, we consider the following situation.

- A is an abelian variety over $\mathbb{Q}$ (for simplicity, we could work over a number field instead);
- $X \subset A$ is a closed subvariety not containing any translates of subabelian varieties of A of positive dimension (this implies that $X(\mathbb{Q})$ is finite);
- We know (explicit generators of) the Mordell-Weil group $A(\mathbb{Q})$.

Of course, the last requirement is highly nontrivial in practice.

The typical situation is when X is a curve of genus $g \geq 2$ embedded into its Jacobian variety A. When $g = 2$, we can determine $A(\mathbb{Q})$ in many cases.

1. The Mordell-Weil Sieve

The idea of the Mordell-Weil Sieve is to combine our 'global' knowledge of $A(\mathbb{Q})$ with 'local' information on how X sits inside A, in order to obtain information on $X(\mathbb{Q})$. The simplest instance uses a finite set S of primes of good reduction for X and A and considers the following diagram.

$$\begin{array}{ccc} X(\mathbb{Q}) & \hookrightarrow & A(\mathbb{Q}) \\ \downarrow & & \downarrow \beta \\ \prod_{p\in S} X(\mathbb{F}_p) & \xhookrightarrow{\alpha} & \prod_{p\in S} A(\mathbb{F}_p) \end{array}$$

If the images of the maps α and β above are disjoint, then $X(\mathbb{Q})$ must be empty.

Conversely, we can ask, if $X(\mathbb{Q})$ is empty, can we expect the images of α and β to be disjoint if S is sufficiently large?

Bjorn Poonen has come up with some heuristic considerations that indicate a positive answer. Roughly, the argument is as follows. Let $B > 0$ be a parameter (which we will choose large later) and let S_B be the set of good primes $p \leq B^2$ such that $\#A(\mathbb{F}_p)$ is B-smooth. We expect $\#S_B \geq \delta\pi(B^2)$ when B is large, for some $\delta > 0$. Then one can work out that

$$\#\prod_{p\in S_B} A(\mathbb{F}_p) \approx e^{\delta B^2 \dim A}, \quad \#\prod_{p\in S_B} X(\mathbb{F}_p) \approx e^{\delta B^2 \dim V}, \quad \#\operatorname{im}(\beta) \approx e^{2rB \dim A},$$

where r is the rank of $A(\mathbb{Q})$. The expected size of $\operatorname{im}(\alpha) \cap \operatorname{im}(\beta)$ is about $e^{2rB \dim A - \delta B^2 \operatorname{codim}_A X}$, which tends to zero very quickly as $B \to \infty$. For details, see [3].

So we have as a **first application** that we can prove $X(\mathbb{Q}) = \emptyset$ for curves X of higher genus (say). The Mordell-Weil sieve was first developed in this context by Scharaschkin [5], who applied it to some twists of the Fermat quartic. It was improved by Flynn [2], who applied it to a number of genus 2 curves, and further improved by Bruin and Stoll [1] in the context of a project which (successfully) aimed at deciding for every genus 2 curve given by an equation

$$y^2 = f_6x^6 + \cdots + f_1x + f_0$$

with integral coefficients $|f_j| \leq 3$ whether it has rational points or not.

2. Improvements and Refinements

In practice, instead of the maps in the diagram above, we compute the maps in the following diagram, with a suitable choice of N.

$$\begin{array}{ccc} X(\mathbb{Q}) & \hookrightarrow & A(\mathbb{Q})/NA(\mathbb{Q}) \\ \downarrow & & \downarrow \beta_N \\ \prod_{p\in S} X(\mathbb{F}_p) & \xrightarrow{\alpha_N} & \prod_{p\in S} A(\mathbb{F}_p)/NA(\mathbb{F}_p) \end{array}$$

We work our way up to this N, by starting with $N_0 = 1$ and multiplying by a prime factor at a time, keeping track of $\beta_N^{-1}(\mathrm{im}(\alpha_N))$ at each stage.

We can use more information than just what we get modulo p for good primes. Instead of looking at the image $X(\mathbb{F}_p)$ of $X(\mathbb{Q}_p)$ in the quotient $A(\mathbb{F}_p)$ of $A(\mathbb{Q}_p)$, we can consider any finite quotient of $A(\mathbb{Q}_p)$ and the image of $X(\mathbb{Q}_p)$ in it. This allows us to use information at bad primes (e.g., we can use the component group), and also information modulo higher powers of p.

In this way, we can restrict our attention to potential rational points on X lying in certain residue classes (even modulo bad primes). We can then use the Mordell-Weil sieve to prove that such points do not exist, even when X does have rational points.

This **second application** proved to be very useful in completing the proof that there are no unknown primitive solutions to $x^2 + y^3 = z^7$, see [4]. There, we had to rule out the existence of rational points satisfying certain congruences mod 2 and 3 on a plane quartic that has rational points and whose Jacobian has Mordell-Weil rank 3.

In a similar way, we can rule out the existence of rational points on X that are in a specified coset of $nA(\mathbb{Q})$ in $A(\mathbb{Q})$, by taking N above to be a multiple of n and restricting to the relevant cosets. This provides a **third application**: if we know a number n such that no two rational points on X are in the same coset mod $nA(\mathbb{Q})$, then we can hope to determine $X(\mathbb{Q})$ — for each coset, we can find a point if one exists and rule out the existence of points if there is no point.

In particular, when X is a curve of genus g and the Mordell-Weil rank of its Jacobian A is less than g, then such an n can be found by Chabauty's approach: if, for every $P \in X(\mathbb{F}_p)$, there is a differential $\omega \in \Omega_X(\mathbb{Q}_p)$ that kills the Mordell-Weil group such that its reduction $\bar{\omega}$ modulo p does not vanish at P, then we can take $n = \#A(\mathbb{F}_p)$. This works very well in practice when $g = 2$ and the rank is 1.

3. Information on Rational Points

When X has rational points and we do not know a number n that 'separates' the points as in the third application above, we still can use the Mordell-Weil sieve in order to obtain information on potential unknown rational points on X. Namely, if all the elements we find in $\beta_N^{-1}(\mathrm{im}(\alpha_N))$ come from known rational points on X, then we can deduce that for every potential unknown point $P \in X(\mathbb{Q})$, there must

be a known $Q \in X(\mathbb{Q})$ such that $P - Q$ is divisible by N in $A(\mathbb{Q})$. This in turn can be translated into a lower bound on the height of any unknown rational point on X, which can be made more or less arbitrarily large.

Combining this with upper bounds obtained using Baker's method, we have as a **fourth application** a way of determining the set of all integral points on a hyperelliptic curve (say), even when its rank is too large to use methods that determine the set of rational points. This is an ongoing project with Bugeaud, Mignotte, Siksek, and Tengely.

References

[1] N. Bruin, M. Stoll, *Deciding existence of rational points on curves: an experiment*, to appear in Experiment. Math.

[2] E.V. Flynn, *The Hasse Principle and the Brauer-Manin obstruction for curves*, Manuscripta Math. **115** (2004), 437–466.

[3] B. Poonen, *Heuristics for the Brauer-Manin obstruction for curves*, Experiment. Math. **15** (2006), 415–420.

[4] B. Poonen, E.F. Schaefer, M. Stoll, *Twists of $X(7)$ and primitive solutions to $x^2 + y^3 = z^7$*, Duke Math. J. **137** (2007), 103–158.

[5] V. Scharaschkin, *Local-global problems and the Brauer-Manin obstruction*, Ph.D. thesis, University of Michigan (1999).

Chabauty for symmetric powers of curves

Samir Siksek

1. Introduction

Let C be a smooth projective absolutely irreducible curve of genus $g \geq 2$ defined over a number field K, and write J for the Jacobian of C. Suppose that the rank of the Mordell–Weil group $J(K)$ is at most $g-1$. In a pioneering paper, Chabauty [1] proved the finiteness of the set of K-rational points on C. This has since been superseded by Faltings' proof of the Mordell conjecture which gives the finiteness of $C(K)$ without any assumption on the rank of $J(K)$. Chabauty's approach however, where applicable, can be refined to obtain explicit bounds for $C(K)$ or even to compute $C(K)$, as in the work of Coleman [2], Grant, McCallum, Flynn, Wetherell, Poonen, Bruin, Stoll, etc.; see [3] for a very useful survey.

One can ask if it is sensible to apply Chabauty to varieties X of dimension at least 2, where the Albanese variety $\mathrm{Alb}(X)$ plays the role of the Jacobian. Of course the Albanese map $\jmath : X \to \mathrm{Alb}(X)$ is often not injective. Indeed $\mathrm{Alb}(X)$ can have smaller dimension than X. However, for varieties X where the Albanese map is injective, or even where $\jmath(X)$ is merely birational to X, there is a hope that Chabauty might enable us to determine the rational points on X. Alas, for a general variety X there are as of yet no algorithms for studying the arithmetic of $\mathrm{Alb}(X)$. A sensible starting point for the investigation of Chabauty in higher dimension is the symmetric powers of curves. Here the Albanese variety is also the Jacobian of the curve.

Our broad objective in this work is to refine the method of Chabauty so that we can compute $C^{(d)}(K)$ in favourable circumstances. Our achievements can be summarized as follows:

(I) Inspired by work of Klassen [4], we give an explicit criterion for an element of $C^{(d)}(K)$ to be the unique element in its residue class, for a given prime v (the residue classes being the fibres of the reduction map). Just as in classical Chabauty, we need an assumption on the rank of the Mordell–Weil group: our criterion requires that $\operatorname{rank} J(K) \leq g - d$.

(II) We often expect, by applying the criterion of (I), to show that the fibres containing a K-rational element do not contain any other. This criterion however does not tell us anything about fibres that do not seem to contain K-rational elements. Thus, if reduction map $C^{(d)}(K) \to C^{(d)}(k_v)$ happens to be surjective then it might be possible to use (I) to show that the known elements of $C^{(d)}(K)$ are the only ones. Experience however suggests that the reduction map is rarely surjective for $d > 1$. To prove that the known elements of $C^{(d)}(K)$ are all its elements, we combine information given by our criterion using several well-chosen primes $v_1, \ldots, v_t$.

(III) Suppose $\varrho : C \to C'$ is a degree d morphism defined over K. Then $\varrho^* C'(K)$ is a subset of $C^{(d)}(K)$. If C' has genus 0 or 1 then $C'(K)$ can be infinite, and in this case $\varrho^* C'(K)$ is an infinite subset of $C^{(d)}(K)$, and undoubtedly, the strategy of (I), (II) fails. In this case we explain how the strategy of (I), (II) can be suitably modified to compute $C^{(d)}(K) \backslash \varrho^* C'(K)$. Again we need a condition on the ranks of the Mordell–Weil groups; in the obvious notation, we require $\operatorname{rank} J_C(K) - \operatorname{rank} J_{C'}(K) \leq g_C - g_{C'} - d + 1$.

We illustrate our method by computing $C^{(2)}(\mathbb{Q})$ for two curves C of genus 3. The first is a hyperelliptic curve, and the second a non-hyperelliptic plane quartic curve. It is noteworthy that in both examples $C^{(2)}$ is a surface of general type, being birational to a Θ-divisor on the Jacobian. Much less is known about the arithmetic of surfaces of general type than that of other surfaces.

We are aware of some earlier Chabauty computations on symmetric squares of hyperelliptic genus 3 curves by Wetherell, although no details of such computations have been published.

2. Examples

2.1. **A Hyperelliptic Example.** Let C be the smooth projective curve over $\mathbb{Q}$ with affine chart

$$C : y^2 = x(x^2 + 2)(x^2 + 43)(x^2 + 8x - 6).$$

Being hyperelliptic, C is of course a double cover of the projective line. In our earlier notation, the map $\varrho : C \to C'$ is just the map

$$C \to \mathbb{P}^1, \qquad (x, y) \mapsto x, \quad \infty \mapsto \infty.$$

Thus

$$\varrho^* \mathbb{P}^1(\mathbb{Q}) = \{\{(x, y), (x, -y)\} \ : \ x \in \mathbb{Q}\} \cup \{\{\infty, \infty\}\}.$$

Note that the hyperelliptic involution $\iota : C \to C$ extends to an involution on $C^{(2)}$ which we will also denote by ι. Thus

$$\iota : C^{(2)} \to C^{(2)}, \qquad \{(x_1, y_1), (x_2, y_2)\} \mapsto \{(x_1, -y_1), (x_2, -y_2)\}.$$

Our method shows that

$$C^{(2)}(\mathbb{Q}) = \varrho^* \mathbb{P}^1(\mathbb{Q}) \cup \{\mathcal{Q}_i : i = 1, \ldots, 10\} \subseteq C^{(2)}(\mathbb{Q}),$$

where

$$\mathcal{Q}_1 = \{(\sqrt{6}, 56\sqrt{6}), (-\sqrt{6}, -56\sqrt{6})\},$$
$$\mathcal{Q}_2 = \{(0,0), \infty\}, \qquad \mathcal{Q}_3 = \{(\sqrt{-2}, 0), (-\sqrt{-2}, 0)\},$$
$$\mathcal{Q}_4 = \{(\sqrt{43}, 0), (-\sqrt{43}, 0)\}, \quad \mathcal{Q}_5 = \{(-4 + \sqrt{22}, 0), (-4 - \sqrt{22}, 0)\},$$
$$\mathcal{Q}_6 = \left\{ \left(\frac{41 + \sqrt{1509}}{2}, -222999 - 5740\sqrt{1509} \right), \text{ conjugate} \right\},$$
$$\mathcal{Q}_7 = \left\{ \left(\frac{-164 + \sqrt{22094}}{49}, \frac{257704352 - 1648200\sqrt{22094}}{823543} \right), \text{ conjugate} \right\},$$
$$\mathcal{Q}_8 = \iota\mathcal{Q}_1, \quad \mathcal{Q}_9 = \iota\mathcal{Q}_6, \quad \mathcal{Q}_{10} = \iota\mathcal{Q}_7.$$

2.2. **A Plane Quartic Example.** Let C be the smooth plane quartic (genus 3) curve with affine equation

$$C : \quad x^4 + (y^2 + 1)(x + y) = 0,$$

and let J be its Jacobian. Schaefer and Wetherell [5] observe that it has a trivial automorphism group, and that its Jacobian J is absolutely simple and not modular. Using a deep descent argument they show that $J(\mathbb{Q}) \cong \mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z}$.

Using our method we showed that $C^{(2)}(\mathbb{Q}) = \{\mathcal{Q}_1, \ldots, \mathcal{Q}_{10}\}$, where

$$\mathcal{Q}_1 = \left\{ (-17 + \sqrt{259}, -48 + 3\sqrt{259}),\ (-17 - \sqrt{259}, -48 - 3\sqrt{259}) \right\},$$
$$\mathcal{Q}_2 = \left\{ \left(-1, \frac{1 + \sqrt{-3}}{2} \right), \left(-1, \frac{1 - \sqrt{-3}}{2} \right) \right\},$$
$$\mathcal{Q}_3 = \left\{ \left(\frac{1 + \sqrt{-3}}{2}, 0 \right), \left(\frac{1 - \sqrt{-3}}{2}, 0 \right) \right\}, \quad \mathcal{Q}_4 = \{(0,0), \infty\},$$
$$\mathcal{Q}_5 = \{(0,0), (0,0)\}, \quad \mathcal{Q}_6 = \{(0,i), (0,-i)\}, \quad \mathcal{Q}_7 = \{(-1,0), \infty\},$$
$$\mathcal{Q}_8 = \{(-1,0), (0,0)\}, \quad \mathcal{Q}_9 = \{(-1,0), (-1,0)\}, \quad \mathcal{Q}_{10} = \{\infty, \infty\}.$$

References

[1] C. Chabauty, *Sur les points rationnels des variétés algébriques dont l'irrégularité est supérieure à la dimension*, C. R. Acad. Sci. Paris **212** (1941), 1022–1024.

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

[3] W. McCallum and B. Poonen, *The Method of Chabauty and Coleman*, available from `http://math.berkeley.edu/~poonen/`

[4] M. J. Klassen, *Algebraic Points of Low Degree on Curves of Low Rank*, Ph.D. dissertation, University of Arizona, 1993.

[5] E. F. Schaefer and J. L. Wetherell, *Computing the Selmer group of an isogeny between abelian varieties using a further isogeny to a Jacobian*, J. Number Theory **115** (2005), no. 1, 158–175.
[6] S. Siksek, *Chabauty for Symmetric Powers of Curves*, submitted.

On the negative Pell equation

Jürgen Klüners
(joint work with Étienne Fouvry)

Let d be a squarefree number and consider the so-called negative Pell equation (NPE):

$$x^2 - dy^2 = -1 \text{ for } x, y \in \mathbb{Z}.$$

Denote by D the discriminant of $\mathbb{Q}(\sqrt{d})$ and by ϵ_D the fundamental unit of the maximal order. Then it is known that NPE(d) is solvable if and only if the fundamental unit ϵ_D has norm -1.

It is clear that the NPE is only solvable when $d > 0$. By reducing modulo a prime $p \mid d$ we get: $x^2 \equiv -1 \bmod p$. The latter equation is only solvable when $p = 2$ or $p \equiv 1 \bmod 4$.

Therefore it is natural to consider the subset of special discriminants:

$$\mathcal{D} := \{D > 0 : D \text{ fundamental}, p \mid D \Rightarrow p \equiv 1, 2 \mod 4\}.$$

Denote by $\mathcal{D}(X) := \#\{D \in \mathcal{D} : D \leq X\}$. Peter Stevenhagen formulates the following conjecture [6]:

Conjecture 1. *Let* $\alpha := \prod_{j=1}^{\infty}(1 + 2^{-j})^{-1} = 0.419422\ldots$ *Then*

$$\lim_{X \to \infty} \frac{\#\{D \in \mathcal{D} : D \leq X \text{ and } \mathrm{Norm}(\epsilon_D) = -1\}}{\mathcal{D}(X)} = 1 - \alpha = 0.580578\ldots$$

It is well known that for a special discriminant D the negative Pell equation is solvable if and only if $\mathrm{Cl}_D = C_D$, i.e. the ordinary and the narrow class group coincide. We remark that for special discriminants the 2–ranks of the two class groups always coincide.

In [2–4] we study the behaviour of the 4–ranks of the class group. Theoretically it is known that these 4–ranks are the same or differ by 1. The behaviour of p–ranks of class groups is predicted by the Cohen–Lenstra heuristics [1] which was extended to 4–ranks by Gerth [5]. In the following we need the function:

$$\alpha_\infty(r) := \frac{\alpha}{\prod_{j=1}^{r}(2^j - 1)}.$$

We are able to prove that the densities

$$\delta(a, b) := \lim_{X \to \infty} \frac{\#\{D \in \mathcal{D} : D < X, \mathrm{rk}_4(\mathrm{C}_D) = a \text{ and } \mathrm{rk}_4(\mathrm{Cl}_D) = b\}}{\mathcal{D}(X)}$$

exist and are equal to:

$$\delta(a,b) = \begin{cases} 0 & \text{if } 0 \le a < b, \\ 0 & \text{if } 0 \le b < a-1, \\ 2^{-a} \cdot \alpha_\infty(a) & \text{if } a = b, \\ (1-2^{-a}) \cdot \alpha_\infty(a) & \text{if } a = b+1. \end{cases}$$

Using the above mentioned results we can control the 4–ranks of those groups. We use the following well known statements:

(1) Let $D \in \mathcal{D}$ such that $\mathrm{rk}_4(C_D) = 0$. Then the negative Pell equation for D is solvable.
(2) Let $D \in \mathcal{D}$ such that $\mathrm{rk}_4(C_D) \neq \mathrm{rk}_4(\mathrm{Cl}_D)$. Then the negative Pell equation for D is not solvable.

Denote by $\mathcal{D}^-(X)$ the number of $D \in \mathcal{D}$ with $D \le X$ such that ϵ_D has norm -1. Then we can prove

Theorem 1. *For $X \to \infty$, we have the inequalities*

$$(\alpha - o(1))\,\mathcal{D}(X) \le \mathcal{D}^-(X) \le \left(\frac{2}{3} + o(1)\right)\,\mathcal{D}(X).$$

We can summarize our result in familiar words as follows: *Stevenhagen conjectures that about 58% of the special D satisfy* $\mathrm{Norm}(\epsilon_D) = -1$. *We prove that this percentage is between 41% and 67%.*

References

[1] H. Cohen and H. W. Lenstra, Jr., *Heuristics on class groups of number fields*, In: Number theory, Noordwijkerhout 1983, volume 1068 of *Lecture Notes in Math.*, pages 33–62. Springer, Berlin, 1984.
[2] É. Fouvry and J. Klüners, *Cohen–Lenstra heuristics of quadratic number fields*, In : F. Hess, S. Pauli, and M. Pohst (ed.) ANTS Proceedings Berlin, LNCS **4076** (2006), 40–55.
[3] É. Fouvry and J. Klüners, *On the 4–rank of class groups of quadratic number fields*, Inv. Math. **167**, (2007), 455–513.
[4] É. Fouvry and J. Klüners, *On the negative Pell equation*, Preprint, 2007.
[5] F. Gerth, III, *Extension of conjectures of Cohen and Lenstra*, Exposition. Math. **5(2)**, (1987) 181–184.
[6] P. Stevenhagen, *The number of real quadratic fields with units of negative norms*, Experiment. Math. **2**, (1993) 121–136.

Statistics for low-lying zeros of Hecke *L*-functions in the level aspect

Guillaume Ricotta

1. Introduction

We would like to provide evidence for the fact that zeros of L-functions seem to behave statistically as eigenvalues of random matrices of large rank throughout the instance of Hecke L-functions. First, we remind you of Iwaniec-Luo-Sarnak's results on one-level densities for low-lying zeros of Hecke L-functions (see [5]) and Katz-Sarnak's results on one-level densities for eigenvalues of orthogonal random matrices (see [6]). Then, we explain that Hughes and Miller (see [1]) found a new example of a very strange phenomenon discovered by Hughes and Rudnick (see [2]) called mock-Gaussian behavior. These works were carried on by the author and Royer in the context of low-lying zeros of symmetric power L-functions in the level aspect (see [7]).

Acknowledgements. *The author would like to thank Henri Cohen, Hendrik W. Lenstra and Don B. Zagier for inviting him to the Mathematisches Forschungsinstitut Oberwolfach on the occasion of the workshop "Explicit Methods in Number Theory". His visit is financed by the ANR project "Aspects Arithmétiques des Matrices Aléatoires et du Chaos Quantique".*

Notation. *We write $\mathcal{P}$ for the set of prime numbers; the main parameter in this paper is a prime number q, whose name is the* level*, which goes to infinity among $\mathcal{P}$. For any $\nu > 0$, $\mathcal{S}_\nu(\mathbb{R})$ stands for the space of even Schwartz functions Φ whose Fourier transform*

$$\widehat{\Phi}(\xi) := \int_{\mathbb{R}} \Phi(x) e(-x\xi)\, \mathrm{d}x$$

is compactly supported in $[-\nu, +\nu]$.

2. A quick walk in the world of L-functions

2.1. **Hecke L-functions and their zeros.** Let f be a primitive cusp form of level q, even integer weight $\kappa \geq 2$ and trivial character ϵ_q say $f \in H_\kappa^*(q)$ (see [3] for the automorphic background). If $(\lambda_f(n))_{n\geq 1}$ are its (suitably normalised) Hecke eigenvalues then we define

$$L(f,s) := \sum_{n\geq 1} \frac{\lambda_f(n)}{n^s} = \prod_{p\in\mathcal{P}} \left(1 - \frac{\lambda_f(p)}{p^s} + \frac{\epsilon_q(p)}{p^{2s}}\right)^{-1},$$

which is an absolutely convergent and non-vanishing Dirichlet series and Euler product on $\Re s > 1$, and also $L_\infty(f,s) := \Gamma_{\mathbb{R}}(s + (\kappa-1)/2)\, \Gamma_{\mathbb{R}}(s + (\kappa+1)/2)$ where $\Gamma_{\mathbb{R}}(s) := \pi^{-s/2}\, \Gamma(s/2)$ as usual. The function $\Lambda(f,s) := q^{s/2} L_\infty(f,s) L(f,s)$ is a *completed L-function* in the sense that it satisfies the following *nice* analytic properties, proved by E. Hecke:

- the function $\Lambda(f,s)$ can be extended to a holomorphic function of order 1 on $\mathbb{C}$;

- the function $\Lambda(f,s)$ satisfies a functional equation of the shape
$$\Lambda(f,s) = i^{\kappa}\epsilon_f(q)\Lambda(f,1-s)$$
where $\epsilon_f(q) = -\sqrt{q}\lambda_f(q) = \pm 1$.

Let us recall some preliminary facts on zeros of Hecke L-functions, which can be found in section 5.3 of [4]. If $\epsilon_f(q) = -1$ then the functional equation of $L(\mathrm{Sym}^r f, s)$ evaluated at the critical point $s = 1/2$ provides a trivial zero. The *Generalised Riemann Hypothesis* is the main conjecture about the horizontal distribution of the zeros of $\Lambda(\mathrm{Sym}^r f, s)$ in the critical strip.

Hypothesis GRH. *For any prime number q and any f in $H_\kappa^*(q)$, all the zeros of $\Lambda(f,s)$ lie on the critical line $\{s \in \mathbb{C}\colon \Re s = 1/2\}$.*

Under hypothesis GRH, it can be shown that the spacing between two consecutive zeros with imaginary part in $[0,1]$ is roughly of size $(2\pi)/\log(q)$. Thus, we normalise the zeros by defining
$$\widehat{\rho} := \frac{\log(q)}{2i\pi}\left(\Re\rho - \frac{1}{2} + i\Im\rho\right)$$
for any zero ρ of $\Lambda(f,s)$. We aim at studying the local distribution of the zeros of $\Lambda(f,s)$ in a neighborhood of the real axis of size $1/\log q$.

2.2. **One-level density.** Fix $\Phi \in \mathcal{S}_\nu(\mathbb{R})$. Let us define the *harmonic* probability measure on $H_\kappa^*(q)$. If A is any subset of this space then its *harmonic probability measure* is defined by
$$\mu_q^h(A) := \sum_{f\in A}\omega_f(q)$$
where the *harmonic weight* associated to any f in $H_\kappa^*(q)$ is given by
$$\omega_q(f) := \frac{\Gamma(\kappa-1)}{(4\pi)^{\kappa-1}\langle f,f\rangle_q}$$
and $\langle f,f\rangle_q$ stands for the Petersson scalar product. The random variable on $\left(H_\kappa^*(q), \mu_q^h\right)$ defined by
$$\forall f \in H_\kappa^*(q), \quad D_{1,q}[\Phi](f) := \sum_{\rho,\Lambda(f,\rho)=0}\Phi\left(\widehat{\rho}\right)$$
is the *one-level density* (relatively to Φ). Its *harmonic expectation* is
$$\mathbb{E}_q^{\mathrm{h}}\left(D_{1,q}[\Phi]\right) := \sum_{f\in H_\kappa^*(q)}\omega_q(f)D_{1,q}[\Phi](f)$$
and its *m-th moments* are
$$\mathbb{M}_{q,m}^{\mathrm{h}}\left(D_{1,q}[\Phi]\right) := \mathbb{E}_q^{\mathrm{h}}\left(\left(D_{1,q}[\Phi] - \mathbb{E}_q^{\mathrm{h}}\left(D_{1,q}[\Phi]\right)\right)^m\right)$$
for any integer $m \geq 1$. We may legitimately wonder if the previous sequences of complex numbers converge as q goes to infinity among the primes. If yes, the following general notations will be used for their limits $\mathbb{E}_\infty^{\mathrm{h}}\left(D_1[\Phi]\right)$ and $\mathbb{M}_{\infty,m}^{\mathrm{h}}\left(D_1[\Phi]\right)$

for any integer $m \geq 1$. Let $\varepsilon = \pm 1$. The *signed harmonic expectation* of the one-level density is

$$\mathbb{E}_q^{\mathrm{h},\epsilon}\left(D_{1,q}[\Phi]\right) := 2 \sum_{\substack{f \in H_\kappa^\epsilon(q) \\ \epsilon_f(q)=\epsilon}} \omega_q(f) D_{1,q}[\Phi](f)$$

and its *signed m-th moments* are

$$\mathbb{M}_{q,m}^{\mathrm{h},\epsilon}\left(D_{1,q}[\Phi]\right) := \mathbb{E}_q^{\mathrm{h},\epsilon}\left(\left(D_{1,q}[\Phi] - \mathbb{E}_q^{\mathrm{h},\epsilon}\left(D_{1,q}[\Phi]\right)\right)^m\right)$$

for any integer $m \geq 1$. The possible limits of these sequences will be denoted $\mathbb{E}_\infty^{\mathrm{h},\epsilon}\left(D_1[\Phi]\right)$ and $\mathbb{M}_{\infty,m}^{\mathrm{h},\epsilon}\left(D_1[\Phi]\right)$ for any integer $m \geq 1$.

3. A very quick walk in the world of random matrices

3.1. **On classical compact groups.** Let $N \geq 1$ be an integer. We define

$$\begin{aligned} U_N &:= \left\{A \in M_N(\mathbb{C}), \quad AA^* = 1_N\right\}, \\ SO_N &:= \left\{A \in U_N \cap M_N(\mathbb{R}), \quad \det(A) = +1\right\} \end{aligned}$$

where 1_N is the identity matrix of size N. These compact groups are endowed with normalised Haar measures d_{U_N} and d_{SO_N}. We consider the following sequences of probability spaces

$$\begin{aligned} O &:= \left((SO_N, \mathrm{d}_{SO_N})\right)_{N\geq 1}, \\ SO^+ &:= \left((SO_{2N}, \mathrm{d}_{SO_{2N}})\right)_{N\geq 1}, \\ SO^- &:= \left(\left(SO_{2N+1}, \mathrm{d}_{SO_{2N+1}}\right)\right)_{N\geq 1}. \end{aligned}$$

Note that the eigenvalues of any $A \in U_N$ can be writen as

$$\exp\left(i\theta_1(A)\right), \ldots, \exp\left(i\theta_N(A)\right)$$

where $0 \leq \theta_1(A)) \leq \ldots \leq \theta_N(A)) \leq 2\pi$. We define the normalised eigenangles by

$$\forall i \in \{1, \ldots, N\}, \quad \widehat{\theta}_j(A) := \frac{N}{2\pi}\theta_i(A).$$

since the mean spacing between eigenangles is roughly $(2\pi)/N$.

3.2. **One-level density.** Fix $\Phi \in \mathcal{S}_\nu(\mathbb{R})$. If $K_N \subset U_N$ is one of the above compact groups, then the random variable on (K_N, d_{K_N}) defined by

$$\forall A \in K_N, \quad D_{1,K_N}[\Phi](A) := \sum_{j=1}^N \Phi\left(\widehat{\theta}_j(A)\right)$$

is the *one-level density* (relatively to Φ). Its *expectation* is

$$\mathbb{E}_{\mathrm{N}}(D_{1,K_N}[\Phi]) := \int_{K_N} D_{1,K_N}[\Phi](A)\mathrm{d}_{K_N}(A)$$

and its *m-th moments* are

$$\mathbb{M}_{\mathrm{N,m}}(D_{1,K_N}[\Phi]) := E_N\left(\left(D_{1,K_N}[\Phi] - E_N(D_{1,K_N}[\Phi])\right)^m\right)$$

for any integer $m \geq 1$. The limits of the sequences of complex numbers

$$\left(\mathbb{E}_{\mathrm{N}}\left(D_{1,K_N}[\Phi]\right)\right)_{N\geq 1}, \quad \left(\mathbb{M}_{\mathrm{N,m}}\left(D_{1,K_N}[\Phi]\right)\right)_{N\geq 1}$$

as N goes to infinity will be denoted

$$\mathbb{E}_{\infty}\left(D_{1,K}[\Phi]\right), \quad \mathbb{M}_{\infty,m}\left(D_{1,K}[\Phi]\right)$$

for any integer $m \geq 1$.

4. Iwaniec-Katz-Luo-Sarnak's results on one-level densities

Katz and Sarnak (see [6]) proved the following result.

Theorem 1. *If $\nu > 0$ is any real number and Φ belongs to $\mathcal{S}_\nu(\mathbb{R})$ then*

$$\begin{aligned}
\mathbb{E}_{\infty}\left(D_{1,O}[\Phi]\right) &= \delta_0(x) + \frac{1}{2}, \\
\mathbb{E}_{\infty}\left(D_{1,SO^+}[\Phi]\right) &= \delta_0(x) + \frac{1}{2}\eta(x), \\
\mathbb{E}_{\infty}\left(D_{1,SO^-}[\Phi]\right) &= \delta_0(x) - \frac{1}{2}\eta(x) + 1,
\end{aligned}$$

where

$$\eta(x) := \begin{cases} 1 & \text{if } |x| < 1, \\ \frac{1}{2} & \text{if } x = \pm 1, \\ 0 & \text{otherwise.} \end{cases}$$

Remark 2. *It should be mentioned that if Φ belongs to $\mathcal{S}_\nu(\mathbb{R})$ with $\nu < 1$ then the three densities match:*

$$\mathbb{E}_{\infty}\left(D_{1,O}[\Phi]\right) = \mathbb{E}_{\infty}\left(D_{1,SO^+}[\Phi]\right) = \mathbb{E}_{\infty}\left(D_{1,SO^-}[\Phi]\right).$$

A result similar in the world of L-functions was proved by Iwaniec and Luo and Sarnak (see [5]).

Theorem 3. *If $\nu < 2$ and Φ is in $\mathcal{S}_\nu(\mathbb{R})$ then*

$$\begin{aligned}
\mathbb{E}^{\mathrm{h}}_{\infty}\left(D_1[\Phi]\right) &= \mathbb{E}_{\infty}\left(D_{1,O}[\Phi]\right), \\
\mathbb{E}^{\mathrm{h},+1}_{\infty}\left(D_1[\Phi]\right) &= \mathbb{E}_{\infty}\left(D_{1,SO^+}[\Phi]\right), \\
\mathbb{E}^{\mathrm{h},-1}_{\infty}\left(D_1[\Phi]\right) &= \mathbb{E}_{\infty}\left(D_{1,SO^-}[\Phi]\right).
\end{aligned}$$

Remark 4. *The crucial fact is that the authors succeeded in breaking the natural barrier $\nu = 1$.*

Remark 5. *This result, which is believed to be true without any restriction on the size of the support ν, suggests that zeros of Hecke L-functions behave like eigenvalues of orthogonal random matrices of large rank. In addition, a trivial vanishing at the critical point seems to have some effect on the behaviour of low-lying zeros.*

5. Hughes-Miller's results on mock-Gaussian behaviour

For any $\Phi \in \mathcal{S}_\nu(\mathbb{R})$, one defines

$$\sigma_\Phi^2 := 2\int_{-1}^{+1} |u|\widehat{\Phi}^2(u)\,\mathrm{d}u$$

and

$$R_m(\Phi) := (-1)^{m-1}2^{m-1}\left(\int_{\mathbb{R}} \Phi(x)^m \frac{\sin(2\pi x)}{2\pi x}\,\mathrm{d}x - \frac{1}{2}\Phi(0)^m\right)$$

for any integer $m \geq 1$. Hughes and Miller proved the following striking result (see [2]).

Theorem 6. *Let $\varepsilon = \pm 1$ and $\Phi \in \mathcal{S}_\nu(\mathbb{R})$. We assume hypothesis* GRH *and the Generalized Riemann hypothesis for all Dirichlet L-functions. If $\nu < \frac{1}{m-1}$ then*

$$\mathbb{M}^{\mathrm{h}}_{\infty,m}\left(D_1[\Phi]\right) = \mathbb{M}_{\infty,m}\left(D_{1,0}[\Phi]\right) = \begin{cases} 0 & \text{if } m \text{ is odd,} \\ 2\int_{\mathbb{R}}|u|\widehat{\Phi}^2(u)\,\mathrm{d}u \times \frac{m!}{2^{m/2}\left(\frac{m}{2}\right)!} & \text{otherwise.} \end{cases}$$

and

$$\mathbb{M}^{\mathrm{h},\epsilon}_{\infty,m}\left(D_1[\Phi]\right) = \mathbb{M}_{\infty,m}\left(D_{1,S0^\varepsilon}[\Phi]\right) = \begin{cases} \varepsilon \times R_m(\Phi) & \text{if } m \text{ is odd,} \\ \varepsilon \times R_m(\Phi) + 2\int_{\mathbb{R}}|u|\widehat{\Phi}^2(u)\,\mathrm{d}u \times \frac{m!}{2^{m/2}\left(\frac{m}{2}\right)!} & \text{otherwise.} \end{cases}$$

Remark 7. *It may be checked that if $\nu < \frac{1}{m}$ then $R_m(\Phi) = 0$ while if $\nu < \frac{1}{m-1}$ then $R_m(\Phi)$ is not identically zero. As a consequence, the moments of the signed one-level densities of low-lying zeros of Hecke L-functions and the moments of the one-level densities attached to SO^- and SO^+ are Gaussian if $\nu < \frac{1}{m}$ but cease to be Gaussian as soon as the support exceeds $\frac{1}{m}$. Such a phenomenon was observed for the first time by Hughes and Rudnick (see [2]) in the particular case of Dirichlet L-functions. In addition, the defect of being Gaussian is exactly balanced according to the "sign", which implies that the moments of the one-level density of low-lying zeros of Hecke L-functions and the moments of the one-level density attached to O are Gaussian if $\nu < \frac{1}{m}$.*

Remark 8. *Let us explain the different assumptions in the previous theorem. Firstly, hypothesis* GRH *may be easily removed. Secondly, the Generalized Riemann hypothesis for all Dirichlet L-functions is crucial for the following reason. The Gaussian term comes from the diagonal term in Petersson's trace formula whereas the non-Gaussian term $R_m(\Phi)$ comes from an analysis of sums of Kloosterman sums on the prime numbers. Evaluating such sums comes down to evaluating sums of characters over the prime numbers.*

References

[1] C. P. Hughes and Steven J. Miller, *Low-lying zeros of L-functions with orthogonal symmetry*, Duke Math. J. **136** (2007), no. 1, 115–172. MR MR2271297

[2] C. P. Hughes and Z. Rudnick, *Linear statistics of low-lying zeros of L-functions*, Q. J. Math. **54** (2003), no. 3, 309–333. MR MR2013141 (2005a:11131)
[3] Henryk Iwaniec, *Topics in classical automorphic forms*, Graduate Studies in Mathematics, vol. 17, American Mathematical Society, Providence, RI, 1997. MR MR1474964 (98e:11051)
[4] Henryk Iwaniec and Emmanuel Kowalski, *Analytic number theory*, American Mathematical Society Colloquium Publications, vol. 53, American Mathematical Society, Providence, RI, 2004. MR MR2061214 (2005h:11005)
[5] Henryk Iwaniec, Wenzhi Luo, and Peter Sarnak, *Low lying zeros of families of L-functions*, Inst. Hautes Études Sci. Publ. Math. (2000), no. 91, 55–131 (2001). MR MR1828743 (2002h:11081)
[6] Nicholas M. Katz and Peter Sarnak, *Random matrices, Frobenius eigenvalues, and monodromy*, American Mathematical Society Colloquium Publications, vol. 45, American Mathematical Society, Providence, RI, 1999. MR MR1659828 (2000b:11070)
[7] G. Ricotta and E. Royer, *Statistics for low-lying zeros of symmetric power l-functions in the level aspect*, preprint available at `http://arxiv.org/abs/math/0703760` (2007).

Double zeta values and modular forms

Herbert Gangl
(joint work with Masanobu Kaneko and Don Zagier)

The *double zeta values*, which are defined for integers $r \geq 2$, $s \geq 1$, by

$$\zeta(r,s) \;=\; \sum_{m>n>0} \frac{1}{m^r n^s}\,, \tag{1}$$

are subject to numerous relations. Already Euler found that when the weight $k = r + s$ is odd the double zeta values can be reduced to products of usual zeta values. Furthermore, he gave the sum formula

$$\sum_{r=2}^{k-1} \zeta(r, k-r) \;=\; \zeta(k) \qquad (k > 2). \tag{2}$$

The aims of the talk were to give other interesting relations among double zeta values, and to indicate that the structure of the $\mathbb{Q}$-vector space of all relations among double zeta values of weight k is connected with the structure of the space of modular forms M_k of weight k on the full modular group $\Gamma_1 = \mathrm{PSL}(2,\mathbb{Z})$.

Double zeta values are a special case of *multiple zeta values*, defined by sums like (1) but with longer decreasing sequences of integers, which are known to satisfy a collection of relations called the *double shuffle relations*. The specialization of these relations to the double zeta case is given by the following two sets of easily proved relations:

$$\zeta(r,s) + \zeta(s,r) = \zeta(r)\,\zeta(s) - \zeta(k) \qquad (r+s=k;\ r,s \geq 2)\,,$$

$$\sum_{r=2}^{k-1} \left[\binom{r-1}{j-1} + \binom{r-1}{k-j-1} \right] \zeta(r,k-r) = \zeta(j)\,\zeta(k-j) \qquad (2 \leq j \leq \frac{k}{2})\,. \tag{3}$$

We wish to study the relations which can be deduced from (3). Since we want to do this algebraically, it is useful to work, not with the double zeta values themselves,

which for all we know may satisfy other relations than (3) (it is not even known that any $\zeta(r,s)/\pi^{r+s}$ is irrational), but with the *formal double zeta space* $\mathcal{D}_k$, generated by formal symbols $Z_{r,s}$, $P_{r,s}$ and Z_k subject to the relations (3), with $Z_{r,s}$, $P_{r,s}$ and Z_k taking the role of $\zeta(r,s)$, $\zeta(r)\zeta(s)$ and $\zeta(k)$, respectively, and where r and s are allowed to assume the value 1.

In $\mathcal{D}_k$ we can prove a number of explicit relations. In particular, Euler's result that all $Z_{r,s}$ are rational linear combinations of the $P_{r,s}$ when the weight k is odd holds in the formal double zeta space $\mathcal{D}_k$, so that we can (and usually will) assume that k is even. Similarly, the formal analogue of Euler's sum formula (2) holds in $\mathcal{D}_k$, and in fact (for k even) has a refinement giving the sums of the even- and odd-argument double zeta values of weight k separately. Surprisingly, they are always in the ratio 3:1, independently of k:

Theorem 1. *For even $k>2$, one has*

$$\sum_{\substack{r=2\\ r\text{ even}}}^{k-1} Z_{r,k-r} = \frac{3}{4}\,Z_k\,, \qquad \sum_{\substack{r=2\\ r\text{ odd}}}^{k-1} Z_{r,k-r} = \frac{1}{4}\,Z_k\,.$$

As an example of a more complicated identity, we show that, for $m,n\ge 1$ odd, $m+n=k>2$,

$$2\sum_{\nu=0}^{n-1}\binom{-m}{\nu}B_\nu\,Z_{n-\nu,m+\nu} = \sum_{r+s=k}(-1)^{s-1}\lambda_{m,n}(r,s)P_{r,s}\,,$$

where B_ν is the νth Bernoulli number and

$$\lambda_{m,n}(r,s) = \sum_{\nu=0}^{n-1}\binom{m+\nu-1}{\nu}\binom{r-1}{n-\nu-1}B_\nu$$

(which despite appearances is symmetric in r and s). Since $B_\nu=0$ for all odd ν except $\nu=1$, this implies that any $Z_{\mathrm{ev},\mathrm{ev}}$ can be written in terms of $Z_{\mathrm{od},\mathrm{od}}$'s and $P_{r,s}$'s. But in fact only $Z_{\mathrm{od},\mathrm{od}}$'s are required:

Theorem 2. *Let $k>2$ be even. Then the $Z_{r,k-r}$ with $0<r<k$ odd are a basis of $\mathcal{D}_k$. There are explicit representations of the elements of various bases of $\mathcal{D}_k$ as linear combinations of the $Z_{\mathrm{od},\mathrm{od}}$'s.*

Theorem 2 is false for double zeta values. Instead we have the following result, which gives the first connection with modular forms:

Theorem 3. (Rough statement.) *The values $\zeta(\mathrm{od},\mathrm{od})$ of weight k satisfy at least $\dim S_k$ linearly independent relations, where S_k denotes the space of cusp forms of weight k on Γ_1.*

Example. For $k=12$, the first weight for which there are non-zero cusp forms on Γ_1, we have the identity

$$28\,\zeta(9,3)+150\,\zeta(7,5)+168\,\zeta(5,7) \;=\; \frac{5197}{691}\,\zeta(12) \tag{4}$$

which can be written in terms only of $\zeta(\mathrm{od},\mathrm{od})$'s using Theorem 1.

Although Theorem 3 holds for the "true" double zeta world and is false in the formal one, it is in fact a consequence of a result in the formal space. In fact, it follows from two different—though complementary—results. Both of them involve period polynomials. We recall the definition of these polynomials. For each even k we consider the space V_k of homogeneous polynomials of degree $k-2$ in two variables and the subspace $W_k \subset V_k$ of polynomials satisfying the relations $P(X,Y)+P(-Y,X)=0$, $P(X,Y)+P(X-Y,X)+P(Y,Y-X)=0$. It splits as the direct sum of subspaces W_k^+ and W_k^- of polynomials which are symmetric and antisymmetric with respect to $X \leftrightarrow Y$, with the former being odd and the latter even with respect to $X \mapsto -X$. The Eichler-Shimura-Manin theory tells us that there are canonical isomorphisms over $\mathbb{C}$ between S_k and W_k^+ and between M_k and W_k^-. The full statement of Theorem 3 associates to any polynomial in W_k^-, in an injective way, an explicit relation among the numbers $Z_{\mathrm{od,od}}$ and $P_{\mathrm{ev,ev}}$ (and Z_k). For the above example (4), for instance, the polynomial $X^2Y^2(X^2-Y^2)^3$ in W_{12}^- leads to the relation

$$28\,Z_{9,3}+150\,Z_{7,5}+168\,Z_{5,7} \;=\; 28P_{4,8}+\frac{95}{3}P_{6,6}-\frac{167}{3}Z_{12}\,,$$

which by Euler's theorem agrees with (4) modulo $\mathbb{Q}\pi^{12}$.

The other result about formal double zeta values which implies Theorem 3 involves the space W_k^+ rather than W_k^-. More precisely, it involves a certain 1-dimensional extension $\widehat{W}_k^+ \subset V_k + \mathbb{C}\cdot\big(X^{k-1}Y^{-1}+X^{-1}Y^{k-1}\big)$ (see §6 for details) which is isomorphic to M_k rather than S_k:

Theorem 4. *If $\{Z_{r,s},\, P_{r,s},\, Z_k\}$ is a collection of numbers satisfying the double shuffle relations in weight k, then the polynomial*

$$\sum_{\substack{r+s=k\\ r,\ s\ \text{even}}} P_{r,s}\,X^{r-1}Y^{s-1}\,\frac{Z_k}{2}\,\big(X^{k-1}Y^{-1}+X^{-1}Y^{k-1}\big)$$

belongs to $\widehat{W}_k^+$ (and to W_k^+ if $Z_k=0$). Every element of $\widehat{W}_k^+$ arises in this way.

From one point of view, this says that the subspace $\mathcal{P}_k^{\mathrm{ev}}$ of $\mathcal{D}_k$ spanned by the $P_{r,s}$ with r and s even is canonically dual to $\widehat{W}_k^+$. From another, it says that there are $k/6+\mathrm{O}(1)$ relations among the $P_{\mathrm{ev,ev}}$, these relations being the same as the relations satisfied by the coefficients of period polynomials in W_k^+. Moreover , we also have

Theorem 5. *The space $\mathcal{P}_k^{\mathrm{ev}}$ is canonically isomorphic to $M_k^{\mathbb{Q}}$, by a map which sends $P_{r,s}$ to $(2\pi i)^{-k}G_rG_s$ (plus a multiple of G'_{k-2} if r or $s=2$) and Z_k to $(2\pi i)^{-k}G_k$.*

Lifting this statement to $\mathcal{D}_k$ leads naturally to the definition of *double Eisenstein series* as

$$G_{r,s}(\tau) = \sum_{\substack{\mathbf{m},\,\mathbf{n}\in\mathbb{Z}\tau+\mathbb{Z}\\ \mathbf{m}\succ\mathbf{n}\succ 0}} \frac{1}{\mathbf{m}^r\mathbf{n}^s} \qquad (\tau\in\mathfrak{H}=\text{upper half-plane}),$$

where $\mathbf{n} \succ 0$ means $\mathbf{n} = n\tau + b$ with $n > 0$ or $n = 0, b > 0$ and $\mathbf{m} \succ \mathbf{n}$ means $\mathbf{m} - \mathbf{n} \succ 0$.

They also turn out to satisfy the double shuffle relations. For details, see [1].

References

[1] H. Gangl, M. Kaneko, D. Zagier, *Double zeta values and modular forms*, in: "Automorphic forms and zeta functions", Proceedings of the conference in memory of Tsuneo Arakawa, World Scientific, 2006.

Weyl group multiple Dirichlet series

Paul E. Gunnells
(joint work with Gautam Chinta and Sol Friedberg)

Let Φ be an irreducible, reduced root system of rank r and with Weyl group W. Let θ be a regular weight for Φ. The goal of this talk is to describe the construction of a Dirichlet series in r complex variables $s_1, \dots, s_r$ depending on θ, with meromorphic continuation to $\mathbf{C}^r$, and satisfying a group of functional equations isomorphic to W. Such series have appeared in the literature in different applications. Conjecturally the series we construct are the Fourier–Whitaker coefficients of the Eisenstein series attached to the Borel subgroup of metaplectic covers of split semisimple algebraic group attached to Φ. The series also have many intriguing connections with combinatorics and representation theory.

For example, when $\Phi = A_2$ and θ is the sum of the fundamental weights, such a series has the form

$$Z(s_1, s_2) = \sum_{\substack{d,m>0 \\ d,m \text{ odd}}} \chi_{d_0}(\hat{m}) a(d,m) m^{-s_1} d^{-s_2}, \quad s_i \in \mathbf{C} \tag{1}$$

on the region on absolute convergence. Here d_0 is the squarefree part of d, $\hat{m}$ is the part of m relatively prime to d_0, and χ_l denotes the character attached to the quadratic extension $\mathbf{Q}(\sqrt{l})/\mathbf{Q}$. The function $a(d,m)$ is defined through the multiplicativity relation

$$a(d,m) = \prod_{p^k || d, p^l || m} a(p^k, p^l)$$

and at p by

$$a(p^k, p^l) = \begin{cases} \min(p^{k/2}, p^{l/2}) & \text{if } \min(k,l) \text{ is even,} \\ 0 & \text{otherwise.} \end{cases} \tag{2}$$

This series was essentially constructed by Siegel [11] and was later used by Goldfeld–Hoffstein [10] to study mean values of the form

$$\sum_{|d|>0} L(1/2, \chi_d) \quad \text{and} \quad \sum_{|d|>0} L(1, \chi_d). \tag{3}$$

Note that if we ignore the differences between d_0, d and $\hat{m}, m$, and ignore a, the $Z(s_1, s_2)$ roughly has the form

$$Z(s_1, s_2) \approx \sum_{d,m>0} \left(\frac{d}{m}\right) m^{-s_1} d^{-s_2} \approx \sum_d L(s_1, \chi_d) d^{-s_2}.$$

This explains the relevance of (1) to investigate sums of the form (3).

The general series is constructed out of nth power residue symbols; the generalization of (2) is constructed using a twisted deformed version of the Weyl character formula. We now give the definition under the simplifying assumptions that Φ is simply-laced and that the symbols are quadratic, i.e. $n = 2$. This is the setting of [7]. The case $\Phi = A_2$ and general n is carried out in [8]. General Φ and general n will be treated in [6].

Let K be a number field with ring of integers $\mathscr{O}$. Let $S = S_f \cup S_\infty$ be a set of places with S_∞ all archimedian places and S_f large enough so that the ring of S-integers $\mathscr{O}_{S_f}$ has class number 1. Let $\mathscr{I}(S)$ be the group of integral ideals prime to S_f, and let $\mathscr{J}(S)$ be the group of fractional ideals coprime with S_f.

There is a quadratic residue symbol $\left(\frac{*}{*}\right) : \mathscr{J}(S) \times \mathscr{J}(S) \to \{-1, 0, 1\}$. Essentially this symbol is defined so that $\left(\frac{(a)}{*}\right)$ gives the character attached to the abelian extension $K(\sqrt{a})$, but there are some technicalities. The full details of this symbol were worked through by Fisher–Friedberg [9].

We choose a subset of positive roots $\Phi^+ \subset \Phi$ and a subset of simple roots $\alpha_1, \ldots, \alpha_r$. Let $\mathbf{s} = (s_1, \ldots, s_r)$ be a vector of r complex variables, indexed by the simple roots in Φ, that is by the nodes of the Dynkin diagram for Φ. Let $\mathbf{I} = (I_1, \ldots, I_r)$ be a tuple of ideals from $\mathscr{I}(S)$, and let $\Psi = (\psi_1, \ldots, \psi_r)$ be a collection of r idèle class characters unramified outside of S. We denote by $\Psi(\mathbf{I})$ the product $\prod_i \psi_i(I_i)$.

We come to our main construction. We define

$$Z_S(\mathbf{s}, \Psi) = \sum_{\mathbf{I} \in \mathscr{I}(S)^r} \frac{\Psi(\mathbf{I}) H(\mathbf{I})}{\prod_j |I_j|^{s_j}}, \tag{4}$$

where $H \colon \mathscr{I}(S)^r \to \mathbf{Z}$ is a function we will specify in a moment. In fact correctly defining H is the main part of the whole story; for Siegel's series ($\Phi = A_2$ and $K = \mathbf{Q}$) H combines $\chi_{d_0}(\hat{m})$ and $a(d, m)$ from (1). The function H is constructed so that $Z_S(\mathbf{s}, \Psi)$ will satisfy r basic functional equations $\sigma_1, \ldots, \sigma_r$, taking $\mathbf{s} = (s_1, \ldots, s_r)$ to $\sigma_{j_0}\mathbf{s} = (s'_1, \ldots, s'_r)$, where

$$s'_j = \begin{cases} s_j + s_{j_0} - 1/2 & \text{if } j \text{ and } j_0 \text{ are adjacent,} \\ 1 - s_{j_0} & \text{if } j = j_0, \text{ and} \\ s_j & \text{otherwise.} \end{cases}$$

Here adjacent means that the variables correspond to adjacent nodes of the Dynkin diagram for Φ. It is easy to check that these involutions generate a group isomorphic to the Weyl group of Φ. Note that H is the *only* part of the definition reflecting the structure of Φ; without it (4) has nothing to do with Φ, except that the number of variables is the same as the rank of Φ.

We first impose on H a *twisted multiplicativity* condition: given ideals $I_j, I'_j \in \mathscr{I}(S)$ with $(I_1 I_2 \cdots I_r, I'_1 I'_2 \cdots I'_r) = 1$ we put

$$\frac{H(I_1 I'_1, \ldots, I_r I'_r)}{H(I_1, \ldots, I_r) H(I'_1, \ldots, I'_r)} = \prod_{\substack{i,j \text{ adj.} \\ i<j}} \left(\frac{I_i}{I'_j}\right)\left(\frac{I'_i}{I_j}\right) \tag{5}$$

Note that if H were actually *multiplicative*, then the right of (5) would be 1. Instead it is a product of symbols reflecting the structure of Φ. This property of H is where the residue symbols appear. Note that since H is not multiplicative, the final series Z_S will not have an Euler product.

Next we define H on tuples of the form $(P^{k_1}, \ldots, P^{k_r})$, where P is a fixed prime ideal, and where the k_i are nonnegative integers. This is the most important part of the construction. Let $\mathbf{x} = (x_1, \ldots, x_r)$ be a vector of variables and let F be the function field $\mathbf{C}(\mathbf{x})$. We define an action of the Weyl group W on F that depends on θ. Then we construct a rational function $f_\theta(\mathbf{x}) \in F$ such that

$$f_\theta(\mathbf{x}) = \sum_{k_1, \ldots, k_r \geq 0} H(P^{k_1}, \ldots, P^{k_r}) x_1^{k_1} \cdots x_r^{k_r} \tag{6}$$

and such that f_θ is invariant under the action and satisfies a few additional technical properties. Using that the local factors of Z are invariant under W we prove that globally Z satisfies the correct functional equations.

For example, for Siegel's series (1) we have

$$f_\theta(x, y) = \frac{1 + x + y - xy^2 - x^2 y - x^2 y^2}{(1 - x^2)(1 - y^2)(1 - p x^2 y^2)}. \tag{7}$$

It is a pleasant exercise to check that under the identification $H(p^k, p^l) = a(p^k, p^l)$, equations (6)–(7) yield (2).

This talk presented joint work with Gautam Chinta and Sol Friedberg on the construction of multiple Dirichet series in several complex variables [5–8]. Related work has been carried out by Ben Brubaker, Dan Bump, Gautam Chinta, Sol Friedberg, and Jeff Hoffstein [1–4].

References

[1] B. Brubaker, D. Bump, G. Chinta, S. Friedberg, and J. Hoffstein, *Weyl group multiple Dirichlet series I*, Multiple Dirichlet Series, Automorphic Forms, and Analytic Number Theory (S. Friedberg, D. Bump, D. Goldfeld, and J. Hoffstein, eds.), Proc. Symp. Pure Math., vol. 75, 2006, pp. 91–114.

[2] B. Brubaker, D. Bump, and S. Friedberg, *Weyl group multiple Dirichlet series. IV.*, submitted.

[3] ———, *Weyl group multiple Dirichlet series. II. The stable case*, Invent. Math. **165** (2006), no. 2, 325–355.

[4] B. Brubaker, D. Bump, S. Friedberg, and J. Hoffstein, *Weyl group multiple Dirichlet series III: Eisenstein series and twisted unstable A_r*, to appear in Ann. Math.

[5] G. Chinta, S. Friedberg, and P. E. Gunnells, *On the p-parts of quadratic Weyl multiple series*, to appear in Crelle.

[6] G. Chinta and P. E. Gunnells, in preparation.

[7] ———, *Weyl group multiple Dirichlet series constructed from quadratic characters*, to appear in Invent. Math.
[8] ———, *Weyl group multiple Dirichlet series of type A_2*, submitted to the Lang memorial volume.
[9] Benji Fisher and Solomon Friedberg, *Double Dirichlet series over function fields*, Compos. Math. **140** (2004), no. 3, 613–630.
[10] D. Goldfeld and J. Hoffstein, *Eisenstein series of* 1/2*-integral weight and the mean value of real Dirichlet L-series*, Invent. Math. **80** (1985), 185–208.
[11] C. L. Siegel, *Die Funktionalgleichungen einiger Dirichletscher Reihen*, Math. Zeitschrift **63** (1956), 363–373.

Theoretical aspects of Maass type form computation

Andrew R. Booker
(joint work with Andreas Strömbergsson)

Algorithms for computing non-holomorphic cusp forms (Maass forms) on $\mathrm{PSL}(2,\mathbb{Z})\backslash\mathbb{H}$ have been investigated since the 1970s. Chief among these is the algorithm of D. Hejhal, which is robust both in the correctness of its results, and in its range of applicability. However, until recently, no example of a Maass form had been rigorously computed, the main difficulty being that the discrete spectrum of Maass forms is imbedded in a continuous spectrum spanned by Eisenstein series. This problem was overcome in [1] by making use of the operator introduced by Lindenstrauss and Venkatesh:

$$\Diamond = 2\cos((\log p)\sqrt{\Delta - 1/4}) - T_p,$$

where p is a suitable prime number and T_p the corresponding Hecke operator. This operator is designed to annihilate the contribution from the continuous spectrum; using it, ten Laplacian eigenvalues were computed and certified correct to over 100 decimal places in [1].

In the talk I described some joint work with Andreas Strömbergsson that goes beyond the simple certification technique of [1]. We show that one can use operators like $\Diamond$ to give a version of Hejhal's algorithm (i.e. using only linear systems of equations based on automorphy relations) for which one can *prove* convergence to cusp forms. One of the main obstacles is to show that for any Maass-Hecke eigenform f of Laplacian eigenvalue $\lambda = 1/4 + r^2$, there is a prime p not too large for which the Hecke eigenvalue λ_p is different from $p^{ir} + p^{-ir}$ (the Hecke eigenvalue of the corresponding Eisenstein series). By standard Rankin-Selberg theory and convexity bounds, this is true for some $p \ll_\varepsilon \lambda^{1/2+\varepsilon}$. To improve on the exponent would require a solution to the subconvexity problem for symmetric square L-functions in the eigenvalue aspect, which is not yet available. However, it turns out that a simple automorphy argument using a lower bound for the constant term of the Eisenstein series (which is essentially the Riemann ζ-function on the line $\Re(s) = 1$) gives $p < \sqrt{\lambda}/2\pi$, which is exactly what is needed to solve the problem at hand.

Once one has an algorithm, as above, for computing a list of discrete Laplace eigenvalues, it remains to show that the list is complete. This arises because of the well-known difficulty in bounding the eigenvalue multiplicity. (More precisely, the discrete spectrum is believed to be simple, but the best known multiplicity bound is $O(\sqrt{\lambda}/\log\lambda)$.) To do this, we followed the model described by Turing for verifying the Riemann hypothesis computationally. The precise input needed is an explicit bound on the average of the error term in Weyl's law. Let $N(t)$ denote the number of discrete eigenvalues $\lambda = 1/4 + r^2$ (counting multiplicity) with $r \in [0, t]$, and

$$S(t) = N(t) - \left(\frac{t^2}{12} - \frac{2t}{\pi}\log\frac{t}{e\sqrt{\frac{\pi}{2}}} - \frac{131}{144}\right).$$

Then, for $T > 1$,

$$-\left(2 + O\left(\frac{1}{\log T}\right)\right)\left(\frac{\pi}{12\log T}\right)^2 \le \frac{1}{T}\int_0^T S(t)\,dt \le \left(1 + O\left(\frac{1}{\log T}\right)\right)\left(\frac{\pi}{12\log T}\right)^2.$$

Here the implied constants may be taken to be 13, though we expect that to improve with more work. This result is proven using the Selberg trace formula and some new results on certain extremal functions. The constant $\frac{\pi}{12}$ in the above is best possible by this method, but is already enough to give satisfactory results. We used it to certify complete the first 2000 eigenfunctions, needing less than 2% extra forms for the certification.

Finally, I discussed briefly how one can apply these techniques to give an algorithm for computing real quadratic class numbers unconditionally (i.e. without relying on GRH to certify the results) in best possible time on average. Basically, one can use the trace formula for Hecke operators to evaluate a sum of the form

$$\sum_{d<X} h(d)w(d),$$

running over all fundamental discriminants d, with a positive weight function w. The sum is expressed in terms of spectral data, i.e. Laplacian and Hecke eigenvalues of Maass forms. Given lower bounds for each $h(d)$ (which can obtained quickly using computations in the class group) and a list of those spectral data, one compares both sides to certify that all computed values of $h(d)$ are correct.

References

[1] A. R. Booker, A. Strömbergsson, A. Venkatesh, *Effective computation of Maass cusp forms*, IMRN vol. 2006, article ID 71281, 34 pages.

The curious fact that $\frac{1}{2}\log 2 < .37$

Harold M. Stark

1. Introduction. This paper represents research still in progress. Let S be any set of positive integers and for $x > 0$, let $N(x, S)$ be the number of integers n in S with $n \leq x$. Let now M be an infinite set of positive integers and S a subset of M. There are unsolved problems in number theory where there is a conjectured asymptotic density,

$$N(x, S) \sim CN(x, M) \quad \text{as } x \to \infty,$$

where C is of the form

$$C = \prod_q (1 - a_q),$$

with the product being over all primes q and the numbers a_q are in the range $0 \leq a_q < 1$ and are sufficiently small so that the product for C is convergent (i.e. $C > 0$). The convergence of the product is equivalent to the convergence of $\sum a_q$.

The heuristics for such a conjecture typically involve, for each prime q, throwing out from M a subset M_q whose density in M is presumed to exist and be a_q, with S making up the set of integers in M which are not in any of the M_q. Sometimes it has not been proved that the M_q have a density, and often even when this is known, the necessary uniformity of estimates of the $N(x, M_q)$ as we go through an inclusion-exclusion argument have not been achieved.

Indeed, in some of the most interesting such problems, it is not even currently known that the set S is infinite. It is for these problems that we propose a simple modification that would lead to positive lower densities for S and require only upper estimates on the $N(x, M_q)$ which we would hope are more easily given than the good lower estimates that would also be needed in any inclusion-exclusion argument. Suppose that we can find a real number x_0 and numbers b_q in the range $1 > b_q > 0$ such that for $x > x_0$ and all q,

$$N(x, M_q) < b_q N(x, M),$$

(presumably for each q, we end up with $b_q \geq a_q$) and such that $\sum b_q$ is convergent. For all $x < x_0$, we would then get

$$N(x, S) > \left[1 - \sum_q b_q\right] \cdot N(x, M), \tag{1}$$

so that S would be infinite if $\sum B_q < 1$. Simple alterations are possible when $\sum B_q \geq 1$ although a finite amount of inclusion-exclusion, say for all $q \leq q_0$, would become necessary.

2. Class-numbers of real quadratic fields. This example is presented in Stark [4]. There are two versions here. Let M be the set of all discriminants of real quadratic number fields and S be the subset of all discriminants of real quadratic fields whose class-number is a power of 2. For each odd prime q, M_q is the subset of M with class-numbers divisible by q. The alternative question lets M' be the set of all prime discriminants of real quadratic fields; S' and M'_q are then the intersections of S and M_q with M'. Since the class-number of a prime discriminant is odd, S' consists of the class number one fields in M'.

The Cohen–Lenstra heuristics [1] predict the two sets S and S' have the same densities in M and M', respectively, where for odd q, the M_q and M'_q are the subsets of M and M' with class-numbers divisible by q and the conjectured values of a_q for odd q are the same in both cases and are given by

$$a_q = 1 - \prod_{j=2}^{\infty}(1 - q^{-j}),$$

and we take $a_2 = 0$. The a_q are quite small ($a_3 = .1598\cdots$, $a_5 = .0495\cdots$, etc.) resulting in $C = .7544\cdots$ and $1 - \sum a_q = .7341\cdots$. Class field theory converts the counting of numbers in M_q and M'_q to the counting of certain totally real fields of degree q. Giving upper estimates for this is currently beyond us.

It is often stated that the heuristics are known for $q = 3$ thanks to the work of Davenport and Heilbronn [2]. However Davenport and Heilbronn provide a weighted average for M_3 and I don't believe that even now it is known that M_3 has a limiting density in M. However, in the Ellenberg–Venkatesh talks, it was stated that the average order of the 3-Sylow subgroups of the class groups for all real quadratic fields of discriminant up to x is $4/3$. This instantly leads to an upper asymptotic estimate of $N(x, M)/6$ for the number of discriminants up to x whose class-numbers are divisible by 3. So, according to our method we could take $b_3 = .17$ for example. I do not know what is known for $q = 3$ when we restrict to prime discriminants.

3. Artin's primitive root conjecture. It is natural to look at other problems that might be amenable to this sort of attack. Artin's primitive root conjecture comes immediately to mind. We take $M = P$, the set of primes, and to avoid entanglements which can change the conjectured constant, we will take S to be the set of primes p such that 2 is a primitive root (mod p). Artin conjectured that S has a density in P with

$$C = .3739\cdots,$$

and with the a_q given for all primes q by

$$a_q = \frac{1}{q(q-1)}.$$

Indeed, under GRH, this was proved by Hooley [3] in 1967.

For a given prime q, let

$$K_q = \mathbf{Q}\left(\exp\left(\frac{2\pi i}{q}\right), 2^{1/q}\right),$$

a normal extension of $\mathbf{Q}$ of degree $q(q-1)$. If 2 is not a primitive root (mod p) for some odd prime p, then there is a prime q which divides $(p-1)$ such that 2 is a q^{th} power (mod p). As Artin noted, this relation between p and q is equivalent to the condition that p splits completely in K_q. The primes p which split completely in K_q form the set M_q. From the start, this conjecture is nicer than the class-number conjecture because we actually know the values of a_q are correct.

Furthermore, we can unconditionally do a finite amount of inclusion-exclusion. Let M' be the set of primes which do not split completely in any K_q with $q \leq q_0$. We know that as $x \to \infty$,

$$N(x, M') \sim C_{q_0} N(x, M)$$

[note: $N(x, M) = \pi(x)$], where

$$C_{q_0} = \prod_{q \leq q_0} (1 - a_q).$$

We choose q_0 large enough such that

$$C < C_{q_0} < C + .001,$$

and further such that

$$\sum_{q > q_0} a_q < .001.$$

As an improvement to (1), we wish to subtract from $N(x, M')$ successively for each $q > q_0$ the number of primes p out to x which split completely in K_q. If necessary, we are willing to estimate a_q's in troubling ranges from above, so that if $b_q \geq a_q$ for all $q > q_0$, we hope to have at least

$$\left(C - \sum_{q > q_0} b_q\right) N(x, M) \leq \left(C - \sum_{q > q_0} a_q\right) N(x, M)$$

primes p out to x for which 2 is a primitive root.

Naturally, we will have to consider several ranges of q individually. Since a prime p splitting completely in K_q must satisfy $p \equiv 1 \pmod{q}$, we needn't consider primes $q \geq x$ at all. The larger $q < x$ is, the more difficult a decent estimate for $N(x, M_q)$ becomes. Before looking at Hooley's paper, a natural starting point would be to consider the range $x^{1/2} < q < x$ and it is this range that led to the title of this paper.

As a prelude to counting the number of primes less than x such that $p - 1$ is divisible by a prime q between $x^{1/2}$ and x, we will just count the number of integers n less than x such that $n - 1$ is divisible by at least one such prime q. In fact, since $q > x^{1/2}$, for an integer n contributing to this count, there can only be one such prime q, as otherwise n would be larger than x. Thus the number of n deserves to be asymptotic to

$$\sum_{x^{1/2} < q < x} \frac{x}{q} = x \left[\log\log(x) - \log\log(x^{1/2}) + o(1)\right] \sim x \log(2).$$

(This is the initial range of the Dickman function $\rho(u)$, in this case for $u = 1/2$. For $u < 1/2$, $\rho(u)$ is more difficult to evaluate because we start getting into inclusion-exclusion arguments.) Under the assumption that the same $\log(2)$ density will occur for primes $p < x$ as integers $n < x$, we expect that the number of primes $p < x$ such that $p-1$ is divisible by a prime q in the range $[x^{1/2}, x]$ is asymptotic to $(x/\log(x))\log(2)$. We propose to throw out from our count $N(x, M')$ all of these primes, but there are two problems here. The first problem is that we are in a range where sieves have difficulty counting primes. The second is that $\log(2) > .37$. The latter problem can be overcome by noting that for $q = 2$, we threw out from $N(x, M)$ the $1/2$ of all primes $\equiv 1$ or $7 \pmod 8$ and so at this point, we only need to throw out those primes $p \equiv 3$ or $5 \pmod 8$ with $p < x$ and $p - 1$ divisible by a prime $q > x^{1/2}$. We expect the number of such primes to be asymptotically $\frac{\log(2)}{2} \cdot \frac{x}{\log(x)}$ and it is this expectation that gave rise to the title of this note since $(1/2)\log(2) = .3465\cdots$.

Since the problem of dealing with $q > x^{1/2}$ is loaded with difficulties, it seems worthwhile to see how Hooley dealt with this range. In fact, Hooley made use of the seemingly more intractable condition that p split completely in K_q in the form that p is thrown out when $2^m \equiv 1 \pmod p$ and $p - 1 = mq$. When q is large, m is small and this allowed Hooley to simultaneously count primes for all small m simultaneously. In this manner, he showed unconditionally that the number of primes p less than x such that $q \mid (p-1)$ with prime $q > x^{1/2}\log(x)$ is $O(x/\log(x)^2)$. Hooley likewise dealt unconditionally with those $p = 1 + mq$ where $x^{1/2}/\log(x)^2 < q < x^{1/2}\log(x)$. In fact Hooley introduced our strategy of just dealing with the primes $p \equiv 1 \pmod q$, but his range of q is sufficiently small that the Brun sieve already puts all such p into the error term. These two interesting unconditional results allow us to shift our range of q from $[x^{1/2}, x]$ down to $[x^{1/4}, x^{1/2}]$ and try to estimate primes $p < x$ such that $p \equiv 3$ or $5 \pmod 8$ and $p-1$ is divisible by at least one prime in the new lower range. But we are now in a region where the large sieve is applicable, and so we get a density $\log(2)/2$ for such primes p. Indeed there is now just enough room to slightly lower the exponent $1/4$ at the lower end $x^{1/4}$ of our range of q.

We can't yet cover the range of q up to $x^{1/4-\epsilon}$ unconditionally, but I am beginning to wonder if this is another of those problems where the obstruction to proving there are infinitely many p such that 2 is a primitive root $\pmod p$ is the possible existence of zeta functions of number fields with non-real zeros very close to $s = 1$.

References

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

[2] H. Davenport and H. Heilbronn, On the density of discriminants of cubic fields II, *Proc. Roy. Soc. London Ser. A* **322** (1971), 405–420.

[3] Christopher Hooley, On Artin's conjecture. *J. Reine Angew. Math.* **225** (1967), 209–220.

[4] H. M. Stark, The Gauss class-number problems, to appear in the Proceedings of the 2005 Gauss–Dirichlet conference in Göttingen.

Elliptic curves and surfaces of high rank, I, II, III

Noam D. Elkies

Over the past two years we have improved several of the (Mordell–Weil) rank records for elliptic curves over $\mathbf{Q}$ and nonconstant elliptic curves over $\mathbf{Q}(t)$. For example, we found the first example of a curve $E/\mathbf{Q}$ with 28 independent points $P_i \in E(\mathbf{Q})$ (the previous record was 24, by R. Martin and W. McMillen 2000), and the first example of a curve over $\mathbf{Q}$ with Mordell–Weil group $\cong (\mathbf{Z}/2\mathbf{Z}) \oplus \mathbf{Z}^{18}$ (the previous rank record for a curve with a 2-torsion point was 15, by Dujella 2002). In these lectures we give some of the background, theory, and computational tools that led to these new records and related applications.

I Context and overview: the theorems of Mordell(–Weil) and Mazur; the rank problem; the approaches of Néron–Shioda and Mestre; elliptic surfaces and Néron specialization; fields other than $\mathbf{Q}$.

II Elliptic surfaces and K3 surfaces: the Mordell–Weil and Néron–Severi groups; K3 surfaces of high Néron–Severi rank and their moduli; an elliptic K3 surface over $\mathbf{Q}$ of Mordell–Weil rank 17. Some other applications of K3 surfaces of high rank and their moduli.

III Computational issues, techniques, and results: slices of Niemeier lattices; finding and transforming models of K3 surfaces of high rank; searching for good specializations. Summary of new rank records for elliptic curves.

I Context and overview.

Mordell (1922) proved that the set $E(\mathbf{Q})$ of rational points of an elliptic curve $E/\mathbf{Q}$ has the structure of an abelian group, and that this group is finitely generated. That is, $E(\mathbf{Q}) \cong T \oplus \mathbf{Z}^r$, where T is a finite abelian group (the *torsion group* of E) and r is the *rank* of E.[1] This raises the basic structural question:

Which groups arise as $E(\mathbf{Q})$ for some elliptic curve $E/\mathbf{Q}$?

Equivalently,

Which ordered pairs (T, r) arise as the torsion and rank of some elliptic curve $E/\mathbf{Q}$?

Mazur's celebrated torsion theorem [Mazur 1977] answers the questions of which torsion groups arise: the cyclic groups of order N for $1 \le N \le 10$ and $N = 12$, and the groups $(\mathbf{Z}/2\mathbf{Z}) \oplus (\mathbf{Z}/2N\mathbf{Z})$ for $1 \le N \le 4$. These are exactly the fifteen groups T for which there is a rational modular curve parametrizing elliptic curves E with an embedding of T into $E(\mathbf{Q})$. It is thus almost immediate that each of these fifteen groups arises infinitely often; the deep part of Mazur's theorem is the proof

[1] Weil later (1928) generalized this from $E/\mathbf{Q}$ to A/K for an arbitrary abelian variety A over a number field K, which is why the group $E(\mathbf{Q})$ and rank r are often called the "Mordell–Weil group" and "Mordell–Weil rank" even in the case covered by Mordell's original result.

that when the modular curve has positive genus it has no rational points other than "cusps" (which parametrize certain degenerate elliptic curves).

This leaves the question of which values of r arise for each of the fifteen possible T. At present this question is hopelessly difficult. It is not even known whether infinitely many r arise; equivalently, whether $\limsup_{E/\mathbf{Q}}(r)$ is infinite for some (all) of those T. As long as this question remains intractable, we also ask for which (T, r_0) can we prove that $\limsup(r) \geq r_0$; this is in some sense a more demanding question than finding large individual values of r, in that proving $\limsup(r) \geq r_0$ requires infinitely many curves, not a single lucky guess.

Our main theme is the use of K3 surfaces of high rank and their moduli to get new records for these questions (and also to obtain some other applications of explicit parametrizations of K3 surfaces). For the remainder of this first lecture we outline how the quest for curves of large rank naturally leads to elliptic surfaces, and illustrate two important earlier approaches to the problem.

Essentially the only technique known for proving lower bounds on $\limsup(r)$ (at any rate the only technique known for $r_0 > 2$) is finding *parametrized families*, that is, infinite families of elliptic curves E together with generically independent points $P_1, \ldots, P_{r_0}$.

Paradigmatic example: given (x_i, y_i) $(i = 1, 2, 3)$, solve the simultaneous linear equations for a_2, a_4, a_6 that make $y_i^2 = x_i^3 + a_2 x_i^2 + a_4 x_i + a_6$ for each $i = 1, 2, 3$. This yields an elliptic curve E with 3 rational points (x_i, y_i). Exercise: they are generically independent (that is, independent when E is considered as an elliptic curve over the field $\mathbf{Q}(x_1, y_1, x_2, y_2, x_3, y_3)$). Hint: *any* quadruple (E, P_1, P_2, P_3) (E some elliptic curve, each P_i on E) arises this way for some x_i, y_i if and only if each $P_i \neq 0$ and $P_i \neq \pm P_j$ for $i \neq j$. [Moreover, we can make x_i, y_i unique by requiring $(x_1, x_2) = (0, 1)$; then (x_3, y_1, y_2, y_3) gives a birational parametrization of the "3-rd power $\mathcal{E}^3$ of the universal elliptic curve".] By a specialization theorem of Néron ([Néron 1952], see also [Serre 1989, Ch.11]), later sharpened by Silverman (more on this below), there are infinitely many choices of $(x_i, y_i) \in \mathbf{Q}^6$ for which P_1, P_2, P_3 remain independent on the curve $E/\mathbf{Q}$. Indeed (and not surprisingly), this is true for "most" rational (x_i, y_i), and infinitely many non-isomorphic curves E arise this way. Hence $\limsup(r) \geq 3$.

One quickly sees ways to improve this beyond rank 3; for instance, use the extended Weierstrass form $y^2 + a_1 xy + a_3 = x^3 + a_2 x^2 + a_4 x + a_6$ (or even the same with $a_0 x^3$ instead of x^3); or, pass a cubic plane curve through 9 "random" points of $\mathbf{P}^2$. These are still not that far from each other, but they do suggest two complementary ways of viewing the task. In general, an elliptic curve over $F(t_1, ..., t_n)$ with several rational points is both:

1) ["à la Mestre"] Polynomial identities (algebra, often ingeniously applied), and

2) ["à la Néron"] An algebraic variety of dimension $n + 1$ equipped with a suitable map to n-dimensional space over F (algebraic geometry).

We next give a short table of record ranks of nonconstant elliptic curves[2] over $\mathbf{Q}(t)$, all but the first and last of whose rows are taken from [Rubin–Silverberg 2002, Table 3] and represent the Mestre-style algebraic approach:

Rank $\geq$	Author(s) and year
8, 9, 10	Néron (1952)
11, 12	Mestre (1991)
13	Nagao (1994)
14	Mestre, Kihara (2000–1)
(15,16,)17,18	NDE (2006–7)

This leap from 14 to 18,[3] and similar improvements for curves with nontrivial torsion, is also the key ingredient (via specialization) of the new record ranks for individual curves over $\mathbf{Q}$. Curiously these improvements are achieved by returning to Néron's geometric viewpoint but applying it to elliptic surfaces at the next level of complexity: elliptic K3 surfaces rather than rational elliptic surfaces. We shall say more about this in the second lecture. First we interpolate some comments about Néron's family, an example of Mestre's identities, and remarks on elliptic curves and surfaces defined over number fields other than $\mathbf{Q}$.

Recall that we obtained rank ≥ 3 by birationally parametrizing *all* elliptic curves E with three rational points P_1, P_2, P_3, a.k.a. the "3-rd power $\mathcal{E}^3$ of the universal elliptic curve"; and observed that some higher powers can be likewise parametrized using other models of elliptic curves, notably the unique cubic curve passing through 9 general points $P_1, \ldots, P_9$ in the plane. This already gives $\limsup(r) \geq 9$, because there are various ways to get a 10th point P_0 that can serve as an origin, such as the 9th base-point of the pencil of cubics through $P_1, ..., P_8$.

For $r = 10$, and thus for larger r, it is no longer possible to completely parametrize $\mathcal{E}^r$ — ultimately because the modular form $\Delta = q\prod_{n=1}^{\infty}(1-q^n)^{24}$ yields a holomorphic 11-form on $\mathcal{E}^{10}$! Nevertheless, Néron used the geometry of cubic curves to find (in effect) rational curves on $\mathcal{E}^{10}$ that give rise to elliptic curves over $\mathbf{Q}(t)$ with 10 generically independent rational points. We describe this construction in some detail because some of the ideas will recur in the more complicated setting of elliptic K3 surfaces.

We follow the exposition in [Shioda 1991]. Start with $P_1, ..., P_8$, and thus also the ninth base-point P_0. Then blowing up $\mathbf{P}^2$ at $P_0, P_1, \ldots, P_8$ gives a birational isomorphism of $\mathbf{P}^2$ with the pencil of cubics through these nine points. Choose $P_0, ..., P_8$ on a *cuspidal* cubic, say $\Gamma : Y^2Z = X^3$, and choose the coordinate t on the pencil so that Γ is the preimage of $t = \infty$. For generic such $P_1, \ldots, P_8$ this surface has no reducible fibers, and so rank 8. Parametrize Γ by $A(u) = (u : 1 : u^3)$, so that $A(u_1), A(u_2), A(u_3)$ are collinear iff $u_1 + u_2 + u_3 = 0$; in particular, the line through $A(u)$ and $A(-u/2)$ is tangent to Γ at $A(-u/2)$. Let D_1, D_2, D_3 be

[2]An elliptic curve over $\mathbf{Q}(t_1, \ldots, t_n)$ is "nonconstant" if it is not isomorphic over $\mathbf{Q}(t_1, \ldots, t_n)$ with a curve over $\mathbf{Q}$. Such a curve of rank r yields nonconstant curves of rank at least r over $\mathbf{Q}(t_1, \ldots, t_m)$ for each positive $m < n$ by specialization, so it is enough to consider $n = 1$.

[3]Ranks 15 and 16 are in parentheses because we proved the existence of such curves in 2006 but did not compute them explicitly.

these tangents for u_1, u_2, u_3. Each D_i meets a generic curve E_t of the pencil at 2 points other than $P_i = A(u_i)$; so we get a "double section": a section defined over a double cover of the t-line. Moreover, each of these double covers is rational, and $t = \infty$ is a branch point. So any two of them give a degree-4 cover of $\mathbf{P}^1$ by a rational curve, and Néron shows that the two new points[4] are independent, giving rank 10 over $\mathbf{Q}(t)$. For each $t \in \mathbf{Q}$ (with finitely many exceptions where E degenerates), we obtain by specialization an elliptic curve $E_t/\mathbf{Q}$ with 10 rational points. Since $E/\mathbf{Q}(t)$ is nonconstant, Néron's specialization theorem yields infinitely many choices of t where these points remain independent and the curves E_t are pairwise non-isomorphic. (Silverman later used the canonical height to construct, given a curve $E/\mathbf{Q}(t)$ and independent rational points $P_1, \ldots, P_n$, an effective bound H such that the specialized points on E_t remain independent for all t not of the form t_0/t_1 with $t_0, t_1 \in \mathbf{Z} \cap [-H, H]$, proving that the set of exceptions to independence is finite and effectively computable. See again [Serre 1989, Ch.11].) Using all three D_i yields rank 11 over the compositum of three rational double covers of $\mathbf{Q}(t)$, all branched at $t = \infty$. This compositum is the function field of an elliptic curve, usually of positive rank and thus giving infinitely many examples of elliptic curves over $\mathbf{Q}$ with 11 rational points. A variation of Néron's specialization theorem, or of Silverman's refinement, then shows that these include infinitely many distinct curves of rank at least 11 over $\mathbf{Q}$.

But this did not quite give a nonconstant elliptic curve of rank ≥ 11 over $\mathbf{Q}(t)$. Such a curve was first constructed in [Mestre 1991], as follows. Suppose we have distinct $x_1, \ldots, x_{12} \in \mathbf{Q}$, polynomials $A_2, A_3 \in \mathbf{Q}(X)$ of degrees at most $2, 3$ respectively, and a monic polynomial $R(X)$ of degree 4 whose graph $Y = R(X)$ intersects the plane cubic curve $C : Y^3 + A_2(X)Y + A_3(X) = 0$ at the 12 points $P_i : (X, Y) = (x_i, R(x_i))$. Then we expect to get rank $12 - 1$ by regarding C as an elliptic curve with origin (say) P_1. Now the condition on the x_i, A_j, and R is equivalent to $\prod_{i=1}^{12}(X - x_i) = R^3 + A_2R + A_3$. The x_i thus uniquely determine R as the principal part of the Taylor expansion at infinity of $\left(\prod_{i=1}^{12}(X - x_i)\right)^{1/3}$, and then we can recover A_2 and A_3 if and only if the X^{-1} coefficient of $\left(\prod_{i=1}^{12}(X - x_i)\right)^{1/3}$ vanishes (in which case A_2, A_3 are unique). That coefficient is a homogeneous quintic $F(x_1, \ldots, x_{12})$, which is also invariant under translation $(x_i) \mapsto (x_i - \xi)$ and thus yields degree-5 hypersurface in $\mathbf{P}^{10}$. This hypersurface contains some obvious rational subvarieties such as the subspace cut out by $x_i + x_{6+i} = 0$ $(1 \leq i \leq 6)$, but this choice makes our 11 points dependent (though it gives C a 2-torsion point and can thus be used to construct elliptic curves of moderately large rank with $T \supseteq \mathbf{Z}/2\mathbf{Z}$). Mestre finds a less obvious rational subvariety of dimension 3 that preserves independence, consisting of arbitrary linear combinations of

[4]Four new points are visible, but the two points in each double section sum to an element of the known rank-8 group.

$(a,a,a,b,b,b,c,c,c,d,d,d)$ and $(b,c,d,a,c,d,a,b,d,a,b,c)$ for fixed a,b,c,d.[5] Variations of this idea were later used by Mestre and others [see table above] to push the record rank over $\mathbf{Q}(t)$ to 14 (and also for other purposes, such as constructing hyperelliptic curves of given genus with many rational points). Moreover, it was the rank-11 family that was used by Mestre, Nagao, Fermigier, Kouya, and Martin-McMillen during 1992–2000 to raise the rank record for individual curves $E/\mathbf{Q}$ from 14 to 15, 17, 19, 20, 21, 22, 23, and finally 24 (see [Dujella 2006a]), even after curves of rank > 11 over $\mathbf{Q}(t)$ were found, because Mestre's curves have simpler coefficients and more parameters, and thus offer greater scope for searching for high-rank specializations.

What of the rank of elliptic curves $E/F(T)$ for general fields F? We exclude the case of a "constant elliptic curve", in which E is isomorphic over $F(T)$ with a fixed elliptic curve E_0/F, because then $E(F(T)) = E_0(F)$ (proof: no nonconstant maps from $\mathbf{P}^1$ to E_0), which can be very large and/or complicated if F is large enough. For nonconstant curves, the geometry of the associated elliptic surface (more on this in the next lecture) yields the result that $E(F(T))$ is finitely generated. The list of possible torsion groups is the same that Mazur proved over $\mathbf{Q}$ together with $(\mathbf{Z}/N\mathbf{Z})^2$ $(N = 3,4,5)$ and $(\mathbf{Z}/3\mathbf{Z}) \oplus (\mathbf{Z}/6\mathbf{Z})$, and the proof is much easier than over $\mathbf{Q}$. But, as with Mordell's theorem for $E/\mathbf{Q}$, the bound on the rank is not uniform. Indeed, when F has characteristic $p > 0$ the rank is unbounded for "isotrivial" curves with constant and supersingular j-invariant [Šafarevič–Tate 1967], and also for non-isotrivial ones [Ulmer 2002]. In characteristic zero, it is not yet known whether the rank of nonconstant elliptic curves over $F(T)$ is unbounded even for $F = \mathbf{C}$; the record is due to Shioda [1992]: the curve $y^2 = x^3 + T^n + 1$ over $\mathbf{C}(T)$ has (trivial torsion and) rank ≤ 68, with equality if and only if $360|n$. Note that even though the curve is defined over $\mathbf{Q}$, most sections are not; for instance, if $3|n$ then $(x,y) = (-\mu T^{n/3}, 1)$ is on the curve for each $\mu \in \mathbf{C}$ such that $\mu^3 = 1$. Still, the generators are all defined over some number field F_0, and it follows by Néron's specialization theorem that there are infinitely many elliptic curve of rank at least 68 over F_0.

II Elliptic surfaces and K3 surfaces.

[This part began with a review of the general setup of elliptic curves E over $F(T)$ for an arbitrary field $F \subset \mathbf{C}$, relating the arithmetic of E with intersection theory on the corresponding elliptic surface $\mathcal{X}$. We do not repeat all of this material here; see for instance [Shioda 1990].]

[5] An extra dimension can be obtained by adding multiples of $(c,d,b,d,a,c,b,d,a,c,a,b)$ and $(d,b,c,c,d,a,d,a,b,b,c,a)$, the latter of which is redundant but highlights the $\mathcal{A}_4$ symmetry. This symmetry suggests the following equivalent construction of the resulting copy of $\mathbf{P}^2 \times \mathbf{P}^2$ in the hypersurface $F_5 = 0$: let V be the irreducible 3-dimensional representation of the alternating group $\mathcal{A}_4$, let $\langle \cdot, \cdot \rangle$ be an $\mathcal{A}_4$-invariant perfect pairing on V, and let v, v' be any vectors in V; then the 12 inner products $\langle v, gv' \rangle$ $(g \in \mathcal{A}_4)$ are coordinates x_i of a point on F_5. This can be verified by regarding $F_5(x_1, \ldots, x_{12})$ as an $\mathcal{A}_4^2$-invariant polynomial on $V \oplus V$ and showing it must vanish identically [NDE 3.vii.1991, unpublished e-mail to J.-F. Mestre].

We assume throught that $\mathcal{X}$ is a minimal Néron model for E. Such a surface $\mathcal{X}$ is birational with an elliptic surface in extended Weierstrass form $y^2+a_1xy+a_3 = x^3 + a_2x^2 + a_4x + a_6$, with each a_i $(i = 1, 2, 3, 4, 6)$ a section of $O(id)$ for some nonnegative integer d (in down-to-earth language, a homogeneous polynomial of degree id in two variables). The smallest such d is the "arithmetic genus" of $\mathcal{X}$. As the name suggests, the description of elliptic surfaces of arithmetic genus d gets more complicated as d increases. When $d = 0$ we have a constant elliptic curve E_0 over $F(T)$ (equivalently, a surface $\mathcal{X} \cong E_0 \times \mathbf{P}^1$). Once $d > 0$, it follows from intersection theory on $\mathcal{X}$, together with the fact that $h^{1,1}(\mathcal{X}) = 10d$, that the Mordell–Weil rank of $E/F(t)$ is at most $10d - 2$. Except for the smallest few d it is not known whether this upper bound can be attained.

When $d = 1$ we say $\mathcal{X}$ is a "rational elliptic surface", because it is birational with $\mathbf{P}^2$, at least over an algebraic closure $\overline{F}$. Néron's surfaces of rank 8 are rational. Since $8 = 10d - 2$ for $d = 1$, this gives the maximal Mordell–Weil rank of a rational elliptic surface. Much more can be said of the geometry and arithmetic of such surfaces, notably Shioda's beautiful work relating rational elliptic surfaces with the invariant theory of the Weyl group of the root lattice E_8 and its root sublattices; but we shall not follow this thread here.

Our main concern is the case $d = 2$, when $\mathcal{X}$ is an "elliptic K3 surface". A K3 surface is a smooth algebraic surface $\mathcal{X}$ with trivial canonical class and $H^1(\mathcal{X}, O_{\mathcal{X}}) = 0$. This is the last case in which an algebraic surface can be elliptic in more than one way; we heavily exploit this flexibility in our analysis and computations.

A key invariant of a K3 surface $\mathcal{X}$ is its *Néron–Severi lattice* $\mathrm{NS}(\mathcal{X}) = \mathrm{NS}_{\overline{F}}(\mathcal{X})$. The Néron–Severi lattice of any compact algebraic surface over F is its Néron–Severi group (divisors defined over $\overline{F}$ modulo algebraic equivalence), equipped with the symmetric integer-valued pairing induced from the intersection pairing on divisors. For a K3 surface, this group is a free abelian group, and the pairing is *even*: $D \cdot D \in 2\mathbf{Z}$ for all $D \in \mathrm{NS}(\mathcal{X})$. Let ρ be the rank of $\mathrm{NS}(\mathcal{X})$. By the index theorem, the pairing is nondegenerate of signature $(1, \rho - 1)$.

If $\mathcal{X}$ is elliptic then $\mathrm{NS}(\mathcal{X})$ contains two distinguished classes defined over F, the fiber f (preimage of any point under the map $T : \mathcal{X} \to \mathbf{P}^1$) and the zero-section s_0. The intersection pairing on the subgroup H they generate is determined by $f \cdot f = 0$, $s_0 \cdot f = 1$, and $s_0 \cdot s_0 = -d = -2$; hence H is isomorphic with the "hyperbolic plane" (i.e., the even unimodular lattice with Gram matrix $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$). Conversely, *any* copy of H in $\mathrm{NS}(\mathcal{X})$ defined over F yields a model of $\mathcal{X}$ as an elliptic surface: one of the generators or its negative is effective, and has 2 independent sections, whose ratio gives the desired map to $\mathbf{P}^1$. (Warning: in general one might have to subtract some base locus to recover the fiber class f.) Moreover, the pair $(\mathrm{NS}(\mathcal{X}), H)$ determines the reducible fibers[6] and Mordell–Weil

[6]Except for the distinctions between Kodaira types I_1 and II (simple node and cusp, neither of which contributes to $\mathrm{NS}(\mathcal{X})$), I_2 and III (either of which contributes A_1), and I_3 and IV (either of which contributes A_2).

group of the elliptic surface over $\overline{F}$. Indeed let N_{ess}, the "essential lattice" of the elliptic surface, be the orthogonal complement of H in $\mathrm{NS}(\mathcal{X})$, with the pairing scaled by -1 to make it positive definite. Let $R \subseteq N_{\mathrm{ess}}$ be the *root lattice* of N_{ess}, the sublattice spanned by the roots (vectors of norm 2) in N_{ess}. This is a direct sum of root lattices A_n ($n \geq 1$), D_n ($n \geq 4$), or E_n ($n = 6, 7, 8$), with each factor indicating a reducible fiber of the corresponding type; and the Mordell–Weil group $E(\overline{F}(T))$ is canonically isomorphic with the quotient group N_{ess}/R. In particular its rank is the difference between the ranks of N_{ess} and R. The rank of N_{ess}, in turn, equals $\rho - 2$, so the Mordell–Weil rank is at most $\rho - 2$, with equality if and only if N_{ess} has no roots; in this case the Mordell–Weil rank over $F(T)$ is also $\rho - 2$ if and only if $\mathrm{NS}(\mathcal{X})$ consists entirely of divisor classes defined over F.

Now ρ is at most $h^{1,1}(\mathcal{X}) = 10d = 20$, whence the upper bound $18 = 20 - 2$ on the Mordell–Weil rank. While a rational surface always has $\rho = h^{1,1}$, for more complicated surfaces the Néron–Severi rank ρ may be strictly smaller. For K3 surfaces over $\mathbf{C}$ the situation is completely described by the Torelli theorem of Piateckii-Shapiro and Šafarevič [1971]. This theorem confirms and refines the following naïve parameter count: there are $9 + 13 - 4 = 18$ parameters for an elliptic K3 surface (the coefficients a_4, a_6 of a narrow Weierstrass model have $8 + 1$ and $12 + 1$ coefficients, and we subtract 4 for the dimension of GL_2 acting on the projective coordinates of the T-line); each free N_{ess} generator, whether in R or the Mordell–Weil group, imposes one condition and thus reduces the dimension of the moduli space by 1. Recall that over $\mathbf{C}$ it is known that $H^2(\mathcal{X}, \mathbf{Z}) \cong \mathrm{II}_{3,19}$ (the unique even unimodular lattice of signature $(3, 19)$), and that $\mathrm{NS}(\mathcal{X})$ embeds into $H^2(S, \mathbf{Z})$. The Torelli theorem asserts that this embedding is "optimal", that is, realizes $\mathrm{NS}(\mathcal{X})$ as the intersection of $H^2(\mathcal{X}, \mathbf{Z})$ with a $\mathbf{Q}$-vector subspace of $H^2(\mathcal{X}, \mathbf{Z}) \otimes \mathbf{Q}$; for every such lattice L of signature $(1, \rho - 1)$, there is a nonempty (coarse) moduli space of pairs $(\mathcal{X}, \iota)$, where $\iota : L \to \mathrm{NS}(\mathcal{X})$ is an optimal embedding consistent with the intersection pairing; and each component of the moduli space has dimension $20 - \rho$. Moreover, for $\rho = 20, 19, 18, 17$ these moduli spaces repeat some more familiar ones: CM elliptic curves for $\rho = 20$, elliptic and Shimura modular curves for $\rho = 19$, and moduli of abelian surfaces and RM abelian surfaces for certain cases of $\rho = 17$ and $\rho = 18$. It turns out that many of those moduli spaces are more readily parametrized via K3 surfaces than by more direct approaches. We shall treat these applications elsewhere, concentrating here on the application to elliptic K3 surfaces.

To attain the upper bound of 18 on the Mordell–Weil rank, we must use a model of one of the (countably infinite number of) K3 surfaces of Néron–Severi rank 20 as an elliptic surface with trivial R. This can happen over $\mathbf{C}$, and thus over $\overline{\mathbf{Q}}$ [Cox 1982, Nishiyama 1995]; these proofs via [Piateckii-Shapiro–Šafarevič 1971] use transcendental methods and yield no explicit equations, but the example $Y^2 = X^3 - 27(T^{12} - 11T^6 - 1)$ was later obtained in [Chahal–Meijer–Top 2000]. This still leaves open the question of whether an elliptic K3 surface can have Mordell–Weil rank 18 over $\mathbf{Q}(T)$. We repeat the warning that it is not sufficient for the surface to be defined over $\mathbf{Q}$; as with Shioda's surface $Y^2 = X^3 + T^{360} + 1$, the

Chahal–Meijer–Top surface does not have all of $\mathrm{NS}(\mathcal{X})$ defined over $\mathbf{Q}$. Likewise for the Néron–Severi groups of some other familiar examples of K3 surfaces of maximal Néron–Severi rank, such as the diagonal quartic $X^4 + Y^4 = Z^4 + T^4$ in $\mathbf{P}^3$ or the complete intersection $\sum_{i=1}^6 X_i = \sum_{i=1}^6 X_i^2 = \sum_{i=1}^6 X_i^3 = 0$ in $\mathbf{P}^5$.

One somewhat familiar example where the full Néron–Severi group *is* defined over $\mathbf{Q}$ is the universal elliptic curve with a 7-torsion point, considered naturally as an elliptic surface over the modular curve $X_1(7) \cong \mathbf{P}^1_{\mathbf{Q}}$. But this surface has $|\mathrm{disc}(\mathrm{NS}(\mathcal{X}))| = 7$, much too small for any of its elliptic-surface models to have rank 18. In fact we combine arithmetic considerations with the construction in [Inose 1978] to show that if $\mathrm{NS}_{\mathbf{Q}}(\mathcal{X})$ has rank 20 then $\mathrm{disc}(\mathrm{NS}(\mathcal{X}))$ is one of the thirteen discriminants -3, -4, -7, -8, -11, -12, -16, -19, -27, -28, -43, -67, -163 of imaginary quadratic orders of class number 1. Each of these arises uniquely up to twists, albeit with different elliptic models — already -3 and -4 have 6 and 13 respectively. But even 163 is too small for N_{ess} to have no roots.[7] Therefore there are no elliptic K3 surfaces of Mordell–Weil rank 18 over $\mathbf{Q}$.[8] But Mordell–Weil rank 17 is barely possible — still not with $\big(\rho, |\mathrm{disc}(\mathrm{NS}(\mathcal{X}))|\big) = (20, 163)$ but with an exceptional rational point on a certain Shimura curve!

More on this soon; first we describe torsion on elliptic K3 surfaces. Each of the torsion groups in Mazur's list, other than $\mathbf{Z}/9\mathbf{Z}$, $\mathbf{Z}/10\mathbf{Z}$, $\mathbf{Z}/12\mathbf{Z}$, and $(\mathbf{Z}/2\mathbf{Z}) \oplus (\mathbf{Z}/8\mathbf{Z})$, can arise for such a surface, requiring at least the following reducible fibers, and thus giving an upper bound on the rank equal to 6 less than the number of degenerate fibers counted *without* multiplicity:

torsion	$\{0\}$	$\mathbf{Z}/2\mathbf{Z}$	$\mathbf{Z}/3\mathbf{Z}$	$\mathbf{Z}/4\mathbf{Z}$	$\mathbf{Z}/5\mathbf{Z}$
fibers	1^{24}	$2^8 1^8$	$3^6 1^6$	$4^4 2^2 1^4$	$5^4 1^4$
formula	$(0,0,0,a_4,a_6)$	$(0,a_2,0,a_4,0)$	$(a_1,0,a_3,0,0)$	$(a_1,a_2,a_1a_2,0,0)$	etc.
bound	18	10	6	4	2

torsion	$\mathbf{Z}/6\mathbf{Z}$	$\mathbf{Z}/7\mathbf{Z}$	$\mathbf{Z}/8\mathbf{Z}$
fibers	$6^2 3^2 2^2 1^2$	$7^3 1^3$	$8^2\,4\,2\,1^2$
bound	2	0	0

torsion	$(\mathbf{Z}/2\mathbf{Z}) \oplus (\mathbf{Z}/2\mathbf{Z})$	$(\mathbf{Z}/2\mathbf{Z}) \oplus (\mathbf{Z}/4\mathbf{Z})$	$(\mathbf{Z}/2\mathbf{Z}) \oplus (\mathbf{Z}/6\mathbf{Z})$
fibers	2^{12}	$4^4 2^4$	$6^3 2^3$
bound	6	2	0

The three cases with bound zero are the universal elliptic curves with that torsion group. When the bound is positive it can always be attained over $\mathbf{C}$ but (as was already seen in the case of trivial torsion) might not be attainable

[7] Such a lattice, positive-definite of rank 18 with discriminant 163 and minimal norm ≥ 4, would have broken the density record for a sphere packing in $\mathbf{R}^{18}$. But the existence of such a lattice is not excluded by known sphere-packing bounds, so its impossibility had to be proved by other means.

[8] This was asserted in [Shioda 1994], but as a consequence of an incorrect result that was later retracted.

over $\mathbf{Q}$. The maximal rank is not known yet in each case, because with nontrivial torsion it is possible for the Mordell–Weil group to be defined over $\mathbf{Q}$ even though $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ acts nontrivially on $\mathrm{NS}_{\overline{\mathbf{Q}}}(\mathcal{X})$. Still, the discriminant -163 surface does have an elliptic model that attains rank 4 with torsion group $\mathbf{Z}/4\mathbf{Z}$, and was used to get rank 12 over $\mathbf{Q}$ (the previous rank record for an elliptic curve with a rational 4-torsion point was 9, by Kulesz–Stahlke 2001). Explicitly, the surface has equation $Y^2 + aXY + abY = X^3 + abX^2$ where $(a, b) = ((8T - 1)(32T + 7), 8(T+1)(15T-8)(31T-7))$; it has a 4-torsion point at $X = Y = 0$, and four points with $X = -15(T + 1)(31T - 7)(32T + 7)/4$, $(8T - 1)(15T - 8)(31T - 7)(32T + 7)$, $-(T + 1)(8T - 1)(15T - 8)(32T + 7)$, and $-4(T + 1)(2T + 5)(15T - 8)(32T + 7)$ that together with torsion generate $E(\mathbf{Q}(T))$; and taking $T = 18745/6321$ yields a curve $E/\mathbf{Q}$ with eight further independent points, so $E(\mathbf{Q}) \cong (\mathbf{Z}/4\mathbf{Z}) \oplus \mathbf{Z}^{12}$. There are also various ways to combine pairs of quadratic sections to get infinitely many $E/\mathbf{Q}$ with $E(\mathbf{Q}) \supseteq (\mathbf{Z}/4\mathbf{Z}) \oplus \mathbf{Z}^6$; the previous rank record for an infinite family with 4-torsion was 5 (Kihara 2004, according to [Dujella 2006], where he cites two papers in *Proc. Japan Acad. A*).

A variant approach is to get some of the torsion group by a suitable base change; for instance our records with torsion group $(\mathbf{Z}/2\mathbf{Z}) \oplus (\mathbf{Z}/2\mathbf{Z})$ were obtained by starting from an elliptic K3 surface of Néron–Severi rank 20 with torsion group $\mathbf{Z}/2\mathbf{Z}$ whose remaining 2-torsion points are defined over a quadratic extension of $\mathbf{Q}(T)$ that is still rational; likewise we obtained $(\mathbf{Z}/2\mathbf{Z}) \oplus (\mathbf{Z}/4\mathbf{Z})$ by quadratic base change from a curve over $\mathbf{Q}(T)$ with torsion group $\mathbf{Z}/4\mathbf{Z}$.

We return now to the problem of finding elliptic K3 surfaces of large Mordell–Weil rank with no torsion restriction. Having proved that rank 18 is unattainable, we try for rank 17, corresponding to Néron–Severi rank 19. Here the moduli spaces have dimension $20 - 19 = 1$, and in principle the Torelli theorem for K3 surfaces [Piateckii-Shapiro–Šafarevič 1971] identifies these curves with standard arithmetic quotients. In practice it is not always easy to identify the modular curve corresponding to a given lattice L of signature $(1, 18)$, especially when we need results over $\mathbf{Q}$ rather than $\mathbf{C}$. But some identifications can be made. For instance, If $L \supset \mathrm{II}_{1,17}$ then the surfaces are parametrized by the classical modular curve $X_0(N)/w_N$ where $N = \mathrm{disc}(L)/2$. This curve is rational for some rather large N (largest is 71), and elliptic of rank 1 for some N that are even larger (largest is 131). For $N > 131$ the curve has only finitely many rational points by Mordell-Faltings. We need only one rational point, but it must be neither a cusp (because cusps yield degenerate surfaces) nor a CM point (because CM points yield a surfaces of rank 20). It is expected that there are only finitely many examples; the largest known are for $N = 191$ [Elkies 1998] and $N = 311$ [Galbraith 1999]. But again even those N are too small for N_{ess} to have no roots. Still, $N = 311$ is large enough for R to have rank only 2, leaving Mordell–Weil rank $17 - 2 = 15$. This was already a new record, and as with Néron's construction it could be pushed a bit further with quadratic sections, to 16 over $\mathbf{Q}(T)$ and 17 for infinitely many specializations. (We can increment only once over $\mathbf{Q}(T)$, because for elliptic K3 surfaces we cannot choose the ramification points.) But I

did not compute explicit equations for this K3 surface: such a computation would have been a huge undertaking then, and even now with better tools it would be a substantial project. I did, however, manage to compute an elliptic model for the K3 surface for the $N = 191$ point that has a 2-torsion point and the minimal root lattice A_1^8 that can accommodate $\mathbf{Z}/2\mathbf{Z}$ torsion. Thus this elliptic surface has Mordell–Weil group $(\mathbf{Z}/2\mathbf{Z}) \oplus \mathbf{Z}^9$ over $\mathbf{Q}(T)$. Quadratic sections increment this to 10 over $\mathbf{Q}(T)$ and 11 for an infinite family, improving on Kihara's 2001 and 1997 records of 9 ([Dujella 2006], again citing papers in *Proc. Japan Acad. A*). Specialization of the K3 surface to $t \in \mathbf{Q}$ produced the new record curve $E/\mathbf{Q}$ with $E(\mathbf{Q}) \cong (\mathbf{Z}/2\mathbf{Z}) \oplus \mathbf{Z}^{18}$.

One can do even better when L is an even lattice of signature $(1, 18)$ that does not contain $\mathrm{II}_{1,17}$. Let $N = \mathrm{disc}(L)/2$, and suppose N is squarefree. Then $L \supset \mathrm{II}_{1,17}$ if and only if a certain obstruction in $\mathrm{Br}_2(\mathbf{Q})$ vanishes. This obstruction is supported on an even subset of the prime factors of N. If it does not vanish then we get the corresponding Shimura modular curve instead of a classical (elliptic) modular curve. When N is composite, the Shimura curve can have smaller genus than $X_0(N)/w_N$ because there are fewer oldforms. This lets us use N large enough that N_{ess} can have trivial root system. Even so, we did not find any case where the Shimura curve has infinitely many rational points. But for $N = 6 \cdot 79$ we found a sporadic non-CM point. Here the Shimura curve has genus 2, and a bielliptic involution that lets us predict an equation for the curve using the methods of [González–Rotger 2004]. We find $u^2 = 16t^6 - 19t^4 + 88t^2 - 48$, with the following rational points: the fixed points of the bielliptic involution $(t, u) \leftrightarrow (-t, -u)$, with $t = \infty$; four points with $|t| = 2$ and $|u| = 32$; and four with $|t| = 14/13$ and $|u| = 2^6 251/13^3$. It turns out that the last orbit is non-CM. This one orbit of rational points yields an elliptic K3 surface of Mordell–Weil rank 17 over $\mathbf{Q}(t)$, answering the question in [Shioda 1994] on the maximal Mordell–Weil rank of such a surface. It also yields the new records of 18 for the Mordell–Weil rank of a nonconstant elliptic curve over $\mathbf{Q}(T)$ (again via quadratic base change), and of 19 for a lower bound on $\limsup(r)$ over curves $E/\mathbf{Q}$. Specialization of the rank-17 surface also yields several examples of elliptic curves over $\mathbf{Q}$ with more than 24 independent rational points, including a curve of rank at least 28.

Some remarks on the computation of these families and specializations are in the third lecture. We conclude this second lecture by noting that the connection between K3 surfaces of Néron–Severi rank 19 and Shimura curves also makes it possible to compute explicit information (equations, CM coordinates, Clebsch-Igusa invariants, etc.) about Shimura curves of levels considerably beyond what was previously feasible.

III Computation and results.

We briefly describe the steps of the computations needed to get from the above theory of K3 surfaces and their moduli to explicit elliptic curves over $\mathbf{Q}(T)$ and $\mathbf{Q}$.

Finding suitable positive-definite lattices N_{ess}. After the second lecture's forced march through K3 territory, I thought better of attempting another such review of Euclidean and hyperbolic lattices. Basically N_{ess} is obtained as a suitable slice

of a Niemeier lattice. The Niemeier lattices are the 24 even unimodular lattices Λ of rank 24, each with a known root system R and "glue group" Λ/R, which gives a handle on the torsion and roots of its slices. See [Conway–Sloane 1993, Ch. 10.3, pages 399–402] for an example of this technique.

Finding equations for $E/\mathbf{Q}(T)$ and its Mordell–Weil generators. Here it may seem that we are back where we started: we still seek the coefficients of polynomial identities, such as $y_i(T)^2 = x_i(T)^3 + a_4(T)x_i(T) + a_6(T)$ $(1 \le i \le 17)$, with various auxiliary conditions on the (x_i, y_i) to ensure the correct height pairings. There are too many variables to solve such a nonlinear system directly, but in the 4-torsion case shown earlier it was barely possible. Still it was more convenient to eliminate only some of the variables, and recover the remaining ones as follows. The general theory tells us that the coefficients are rational and behave well modulo suitable small primes p such as $41 = (163 + 1)/4$. An exhaustive search mod p finds a solution. Lift this solution arbitrarily to characteristic zero and regard the lift as a p-adic approximation to the correct solution. Apply the natural generalization of Newton's iteration $x \mapsto x - F(x)/F'(x)$ to this context, using finite differences rather than derivatives to approximate F'. Each step doubles the p-adic precision. Soon the p-adic approximation is close enough to recognize the actual rational numbers by lattice reduction. Then confirm them by substitution into the desired identities. Finally change coordinates to simplify the equations to ones whose coefficients have smaller heights, which is essential for finding high-rank specializations.

Exploiting different elliptic models of the same surface. Simple example: the Inose surfaces $Y^2 = X^3 + AT^4X + B''T^7 + BT^6 + b'T^5$ over the T-line have essential lattice $N_{\text{ess}} = R = E_8^2$ with reducible fibers at $T = 0$ and $T = \infty$. Scaling to $Y^2 = X^3 + AX + B''T + B + B'/T$ we obtain an elliptic model over the X-line, this time with $R = D_{16}$ and $[N_{\text{ess}} : R] = 2$ (note that $(T, Y) = (0, 0)$ is a 2-torsion point). It turns out that the transformation is particularly simple when, as here, the two lattices are "2-neighbors": they have isomorphic index-2 sublattices. We start from a model of $\mathcal{X}$ as an elliptic surface whose coefficients are easier to compute, and then follow a chain of 2-neighbors (and the occasional 3-neighbor) that introduces or removes roots and torsion until it reaches an elliptic surface with the desired essential lattice.

Parametrizing families of K3 surfaces of Néron–Severi rank 19. When the Néron–Severi rank is 19 rather than 20, our task is not to solve for the coefficients of a single surface but to parametrize a one-dimensional family by a modular curve. We start at a known point P_0 of the curve (maybe coming from a surface of rank 20, in an elliptic model in which R is the same but the Mordell–Weil rank is larger by 1), and then deform it p-adically. For example, fix a rational function f of the coefficients (say, the cross-ratio of the T-coordinates of four reducible fibers), and use Newton to find points for which f is near $f(P_0)$. Now the coefficients are generally no longer rational even if $f(P)$ is, but they are algebraic with degree at most $\deg(f)$. We can guess those with lattice reduction if $\deg(f)$ is small enough. Varying $f(P)$ over simple rational numbers in a p-adic neighborhood of $f(P_0)$, we

can then guess the equations relating those coefficients with f by solving simultaneous linear equations. At this point we have a guess for a (usually very singular) model for the moduli curve, and if we can't or won't find a smooth model directly then we can ask Magma (or someday Sage) for it. We then verify that the equations we guessed numerically actually work symbolically. Then specialize to the non-CM point to find the desired surface.

Incrementing the rank via quadratic base change. As already noted, the necessary "quadratic sections" — rational curves on $\mathcal{X}$ that intersect the fiber f with multiplicity 2 — are harder to find than in Néron's situation. The trace of the quadratic section is an element of $E(\mathbf{Q}(T))$, defined mod $2E(\mathbf{Q}(T))$ when we translate by elements of the Mordell–Weil group; equivalently, a half-lattice vector mod $E(\mathbf{Q}(T))$. Intersection theory tells us that we need a coset of $2E(\mathbf{Q}(T))$ in $E(\mathbf{Q}(T))$ consisting of vectors of norm 2 mod 4, with no representatives of norm less than 10. (This is for a surface with no reducible fibers; when $R \neq \{0\}$ the criterion is more complicated.) The corresponding coset of $E(\mathbf{Q}(T))$ in $\frac{1}{2}E(\mathbf{Q}(T))$ then consists of "holes" of norm at least 5/2. For our rank-17 surface, there are literally thousands of such holes, and for each one we get an inequivalent quadratic section. The resulting genus-zero curves are all rational because we can always find some other divisor whose intersection with the quadratic section is odd. This also gives millions of biquadratic base changes of genus 1 and positive rank, any one of which gets the lower bound 19 on $\limsup(r)$. (Alas none of them degenerates to a genus-zero curve, so we do not find an elliptic curve of Mordell–Weil rank at least 19 over $\mathbf{Q}(T)$ this way.)

Guessing good specializations by Mestre's heuristic. The conjecture of Birch and Swinnerton-Dyer suggests that large rank should correlate with small partial products of $L(E,1)$. Taking logarithms, we want to make $\sum_{p<x} \log(p/N_p)$ very negative. Experimentally, we need literally thousands of primes, and must canvass many millions of specializations E_t. That's a lot of N_p's to compute. But each depends only on t mod p, so we precompute $\sum_{p<x} p$ of them once and for all, store a low-precision approximation to $\log(p/N_p)$ for each one, and then search for large values of $\sum_p \log(N_p/p)$ in sieve style.

Finding extra rational points. The resulting candidates for large rank have coefficients much too large for it to be feasible to find new rational points by direct search. The simplest independent set of 28 rational points we could find on our record curve

$$\begin{aligned} y^2 + xy + y = x^3 - x^2 \\ - 2006776241557552658503320820933854275093023031217895650 2 \\ + 3448161179503055646703298569039072 03\ldots \\ \ldots 7485594435931918036126600829629193944873224342 9 \end{aligned}$$

has 28-digit integers for its x-coordinates! When the curve has nontrivial 2-torsion, Cremona's program MWRANK quickly computes Selmer 2-groups to find upper bounds on the rank, and then usually finds enough generators on the candidate

record curves. But in the absence of torsion the coefficients are much too large for descent to be feasible. (This is why we can only say that the curve has rank at least 28, not exactly 28, though it seems quite unlikely that the rank is even larger.) Instead we exploit the known rank-17 sublattice of $E/\mathbf{Q}$ to search for rational points near half-lattice holes of the sublattice. This yields equations $y^2 = Q(x)$ for quartics Q with much smaller coefficients. (This looks close enough to the behavior of 2-descents that the method might be regarded as a fake 2-descent.) We then use a sieve technique, implemented by C. Stahlke and M. Stoll in their C program RATPOINTS, to find a few such rational points near some of the deepest half-lattice holes in the generic Mordell–Weil lattice. Finally we use the canonical height to determine the rank of the subgroup of $E(\mathbf{Q})$ generated by all the known points.

Summary of new rank records. In the following table of record ranks of families of elliptic curves with specified torsion group, "$r+$" means rank at least r over $\mathbf{Q}(T)$, and at least $r+1$ for an infinite family parametrized by a positive-rank elliptic curve obtained by quadratic base change from the record curve over $\mathbf{Q}(T)$. Plain r is a lower bound on the rank of a curve over $\mathbf{Q}(T)$. The previous records as of 2004 are from [Dujella 2006].

torsion	$\{0\}$	$\mathbf{Z}/2\mathbf{Z}$	$\mathbf{Z}/3\mathbf{Z}$	$\mathbf{Z}/4\mathbf{Z}$	$(\mathbf{Z}/2\mathbf{Z}) \oplus (\mathbf{Z}/2\mathbf{Z})$	$(\mathbf{Z}/2\mathbf{Z}) \oplus (\mathbf{Z}/4\mathbf{Z})$
≤ 2004	14	9	6	5	6	3
new	18+	10+	7	5+	7+	3+

For other torsion groups, the records remain 3 for $\mathbf{Z}/5\mathbf{Z}$ and $\mathbf{Z}/6\mathbf{Z}$; "1+" for $\mathbf{Z}/7\mathbf{Z}$, $\mathbf{Z}/8\mathbf{Z}$, and $(\mathbf{Z}/2\mathbf{Z}) \oplus (\mathbf{Z}/6\mathbf{Z})$ (the three cases where the universal elliptic curve is K3); and "0+" for $\mathbf{Z}/9\mathbf{Z}$, $\mathbf{Z}/10\mathbf{Z}$, $\mathbf{Z}/12\mathbf{Z}$, and $(\mathbf{Z}/2\mathbf{Z}) \oplus \mathbf{Z}/8\mathbf{Z}$ (the four cases where the universal elliptic curve has $d > 2$).

The new rank records for individual curves over $\mathbf{Q}$ are as follows:

torsion	$\{0\}$	$\mathbf{Z}/2\mathbf{Z}$	$\mathbf{Z}/4\mathbf{Z}$	$\mathbf{Z}/8\mathbf{Z}$
≤ 2004	24	15	9	5
new	28	18	12	6

torsion	$(\mathbf{Z}/2\mathbf{Z}) \oplus (\mathbf{Z}/2\mathbf{Z})$	$(\mathbf{Z}/2\mathbf{Z}) \oplus (\mathbf{Z}/4\mathbf{Z})$	$(\mathbf{Z}/2\mathbf{Z}) \oplus (\mathbf{Z}/6\mathbf{Z})$
≤ 2004	10	6	5
new	14	8	6

The incremental improvements for torsion groups $\mathbf{Z}/8\mathbf{Z}$ and $(\mathbf{Z}/2\mathbf{Z}) \oplus (\mathbf{Z}/6\mathbf{Z})$ are due only to better searching in known families. The absence (so far?) of a new record for $\mathbf{Z}/3\mathbf{Z}$ may be due to the lack of an efficient implementation of descent via a 3-isogeny.

We conclude with a few remarks on integral points. Our $r \geq 28$ curve has at least 1174 pairs $(x, \pm y)$ of integral points in its minimal model, but this is not a record: a curve with $r \geq 25$ in the same family has at least 2810 such pairs in the known subgroup of $E(\mathbf{Q})$. The same family also contains a curve for which we found only 21 independent points but the subgroup they generate contains at least 2564 pairs of integral points. Over $\mathbf{Q}(T)$, the analogue of integral points

is points (X, Y) where X, Y are polynomials of degree at most $4, 6$ respectively. In the absence of reducible fibers, these are exactly the nonzero elements of the Mordell–Weil group whose canonical height is as small as 4. Our elliptic K3 surface of rank 17 has 1311 such pairs $(X, \pm Y)$.

References

[Chahal–Meijer–Top 2000] J. Chahal, M. Meijer, and J. Top, *Sections on certain $j = 0$ elliptic surfaces*, Comment. Math. Univ. St. Paul. **49** (2000), 79–89.

[Conway–Sloane 1993] J. H. Conway, and N. J. A. Sloane, *Sphere Packings, Lattices and Groups.* New York: Springer 1993.

[Cox 1982] D. A. Cox, *Mordell–Weil groups of elliptic curves over $\mathbf{C}(t)$ with $p_g = 0$ or* 1, Duke Math. J. **49** (1982), 677–689.

[Dujella 2006] A. Dujella, *Infinite families of elliptic curves with high rank and prescribed torsion*, online at http://web.math.hr/~duje/tors/generic.html .

[Dujella 2006a] A. Dujella, *History of elliptic curves rank records*, online at http://web.math.hr/~duje/tors/rankhist.html .

[Dujella 2007] A. Dujella, *High rank elliptic curves with prescribed torsion*, online at http://web.math.hr/~duje/tors/tors.html .

[Elkies 1998] N. D. Elkies, *Elliptic and modular curves over finite fields and related computational issues*, pages 21–76 in Computational Perspectives on Number Theory: Proceedings of a Conference in Honor of A.O.L. Atkin (D.A. Buell and J.T. Teitelbaum, eds.; Providence: American Mathematical Society, 1998).

[Galbraith 1999] S. D. Galbraith, *Rational points on $X_0^+(p)$*, Experimental Math. **8** (1999), 311–318.

[González–Rotger 2004] J. González and V. Rotger, *Equations of Shimura curves of genus two*, International Math. Research Notices **14** (2004), 661–674.

[Inose 1978] H. Inose, *Defining equations of singular K3 surfaces and a notion of isogeny*, pages 495–502 in Proceedings of the International Symposium on Algebraic Geometry (Kyoto Univ., 1977), Tokyo: Kinokuniya Book Store.

[Mazur 1977] B. Mazur, *Modular curves and the Eisenstein ideal*, Inst. Hautes Études Sci. Publ. Math. **47** (1977), 33–186.

[Mestre 1991] J.-F. Mestre, *Courbes elliptiques de rang ≥ 11 sur $\mathbf{Q}(t)$* [Elliptic curves with rank ≥ 11 over $\mathbf{Q}(t)$], C. R. Acad. Sci. Paris, Sér. I (Math.) **313** (1991), 139–142.

[Néron 1952] A. Néron, *Problèmes arithmétiques et géométriques rattachés à la notion de rang d'une courbe algébrique dans un corps*, Bull. Soc. Math. France **80** (1952), 101–166.

[Nishiyama 1995] K.-i. Nishiyama, *Examples of Jacobian fibrations on some K3 surfaces whose Mordell–Weil lattices have the maximal rank* 18, Comment. Math. Univ. St. Paul. **44** (1995), 219–223.

[Piateckii-Shapiro–Šafarevič 1971] I. Piateckii-Shapiro and I. R. Šafarevič, *A Torelli theorem for algebraic surfaces of type K3* [Russian], Izv. Akad. Nauk SSSR, Ser. Mat. **35** (1971), 530–572.

[Rubin–Silverberg 2002] K. Rubin and A. Silverberg, *Ranks of elliptic curves*, Bull. Amer. Math. Soc. (N.S.) **39** (2002), 455–474 (electronic).

[Šafarevič–Tate 1967] I. R. Šafarevič and J. Tate, *The rank of elliptic curves* [Russian], Dokl. Akad. Nauk SSSR **175** (1967), 770–773.

[Serre 1989] J.-P. Serre, *Lectures on the Mordell–Weil Theorem.* Braunschweig: Vieweg, 1989.

[Shioda 1990] T. Shioda, *On the Mordell–Weil lattices*, Comment. Math. Univ. St. Paul. **39** (1990), 211–240.

[Shioda 1991] T. Shioda, *An infinite family of elliptic curves over $\mathbf{Q}$ with large rank via Néron's method*, Invent. Math. **106** (1991), 109–119.

[Shioda 1992] T. Shioda, *Some remarks on elliptic curves over function fields*, Astérisque **209** (1992), 99–114.

[Shioda 1994] T. Shioda, *On the rank of elliptic curves over* $\mathbf{Q}(t)$ *arising from K3 surfaces*, Comment. Math. Univ. St. Paul. **43** (1994), 117–120.

[Ulmer 2002] D. Ulmer, *Elliptic curves with large rank over function fields*, Ann. of Math. (2) **155** (2002), 295–315.

Complexity news: FFT and integer multiplication

Daniel J. Bernstein

URL: `http://cr.yp.to/talks.html#2007.07.18`

- What is the total algebraic complexity of multiplying two polynomials of degree below n over the field of real numbers?

1866	Gauss	FFT	$(15 + o(1))n \lg n$;
1968	Yavne	split-radix FFT	$(12 + o(1))n \lg n$;
News, 2004	Van Buskirk	tangent FFT	$(34/3 + o(1))n \lg n$.

- What is the bit complexity of multiplying two n-bit integers?

1971	Schönhage/Strassen algorithm	$\Theta(n \lg n \lg \lg n)$;
News, 2007	Fürer algorithm	$(n \lg n)2^{O(\lg^* n)}$.

Counting subrings of maximal orders

Jos Brakenhoff

For a number field K of degree n we let $\mathcal{O}_K$ be its ring of integers. We are interested in the number of subrings $R \subset \mathcal{O}_K$ which have a given finite index $[\mathcal{O}_K : R] = h$. I.e., we want to determine

$$f_K(h) = \#\{R \subset \mathcal{O}_K \mid R \text{ is a subring with } [\mathcal{O}_K : R] = h\}.$$

It is well-known that $f_K(h) = 1$ for all number fields of degree 2. Furthermore, results have been obtained for number fields of degree 3 and 4, see for example [1].

The goal of this talk is to give a uniform bound for $f_K(h)$ for number fields of a fixed degree. More precisely, we want to give bounds for

$$F(n) = \lim_{h \to \infty} \frac{\log(f(n,h))}{\log h},$$

where $f(n,h) = \max_{K:deg(K)=n} f_K(n)$, for various n.

This goal is inspired by a question of Manjul Bhargava. He wanted to know whether $F(5)$, and in general $F(n)$, is bounded from above by 2.

We concentrate on the following results.

(1) $F(5) \leq \frac{20}{11} < 2$
(2) $F(13) \geq \frac{35}{17} > 2$
(3) $\limsup_{n \to \infty} \frac{F(n)}{n} \leq 1$
(4) $\liminf_{n \to \infty} \frac{F(n)}{n} \geq (\sqrt{2} - 1)^2$

By localization, we can show that $f(n,h)$ is multiplicative in h. It therefore suffices to bound these values for prime powers $h = p^k$.

Definition 1. *If $G \subset \mathbb{Z}^N$ is a subgroup of index p^k, then $\mathbb{Z}^N/G = \bigoplus_{i=1}^N (\mathbb{Z}/p^{\lambda_i}\mathbb{Z})$ with $k = \sum_{i=1}^N \lambda_i$. Order the λ_i such that $\lambda_1 \le \lambda_2 \le \ldots \le \lambda_N$. The partition $\lambda = (\lambda_1, \lambda_2, \ldots, \lambda_N)$ is called the* type *of G.*

We can determine the number of subgroups of $\mathcal{O}_K$ of given type by Hall polynomials. Given a type $\lambda = (\lambda_1, \ldots, \lambda_N)$, with $\sum_i \lambda_i = k$, there is a monic polynomial $g_\lambda(X) \in \mathbb{Z}[X]$ such that for all $p \in \mathbb{Z}$ prime

$$\#\{G \subset \mathbb{Z}^N \text{ subgroup of index } p^k \text{ and type } \lambda\} = g_\lambda(p).$$

The degree of g_λ is $\sum_{i=1}^N (\lambda_i(2i - N - 1))$.

So the limit behaviour of the number of subgroups of given type is

$$\limsup_{p\to\infty} \frac{\log \#\{G \subset \mathbb{Z}^N \text{ index } p^k, \text{ type } \lambda\}}{\log p^k} = \frac{\sum_{i=1}^N (\lambda_i(2i - N - 1))}{k} = c(\lambda)$$

Example. Take $\lambda_i = 0$ for $i < N$ and $\lambda_N = k$, then

$$c(\lambda) = \frac{k(2N - N - 1)}{k} = N - 1.$$

This is the largest possible value for fixed N.

This example gives us an upper bound for $F(n)$, by counting the number of subgroups which contain 1, i.e., the number of subgroups of $\mathcal{O}_K/\mathbb{Z}$. (Note that $N = n - 1$.) Hence $F(n) \le N - 1 = n - 2$, so we have obtained the third of our results.

By the following lemma we also get a lower bound from counting subgroups.

Lemma 2. *A subgroup G of $\mathcal{O}_K$ that contains 1 for which $G/\mathbb{Z} \subset \mathcal{O}_K/\mathbb{Z}$ is of type $(1, \ldots, 1, 2, \ldots, 2)$ is always a subring.*

A lower bound for $F(n)$ is the maximum of $c(\lambda)$ over all types λ mentioned in the lemma. Set d to be the number of twos in the type. Then $c(\lambda) = \frac{d(n-d-1)}{n+d-1}$, which is maximal when d is close to $(\sqrt{2}-1)(n-1)$. This gives both lower bounds from the results.

For the last of our results, we need to find better bounds for the worst types. Recall that $c(\lambda)$ is maximal when $\lambda_i = 0$ for $i < n-1$ and $\lambda_{n-1} = k$. A subgroup $G \subset \mathcal{O}_K$ of this type satisfies $\mathcal{O}_K/G \cong \mathbb{Z}/p^k\mathbb{Z}$ as groups. We call such subgroups and -rings *co-cyclic*.

Lemma 3. *The maps*

$$\begin{array}{rcl}
\left\{ \begin{array}{cc} R \subset \mathcal{O}_K : & \mathcal{O}_K/R \cong \mathbb{Z}/p^k\mathbb{Z} \\ \text{subring} & \text{as groups} \end{array} \right\} & \to & \left\{ \begin{array}{cc} I \subset \mathcal{O}_K : & \mathcal{O}_K/I \cong (\mathbb{Z}/p^k\mathbb{Z})^2 \\ \text{ideal} & \text{as groups} \end{array} \right\} \\
R & \mapsto & f(R) = \{x \in \mathcal{O}_K : x\mathcal{O}_K \subset R\} \\
g(I) = \mathbb{Z} + I & \leftarrow\!\shortmid & I
\end{array}$$

are each others two-sided inverse.

We obtain a better bound for $\#\{R \subset \mathcal{O}_K$ co-cyclic subring$\}$, since $\#\{I \subset \mathcal{O}_K$ ideal $\mid \mathcal{O}_K/I \cong (\mathbb{Z}/p^k\mathbb{Z})^2\} \leq \binom{n}{2}$.

If $R \subset \mathcal{O}_K$ is a subgroup of index p^k and type λ with $\lambda_{n-1} > 2\lambda_{n-2}$, then

$$R' = \mathcal{O}_K \cap p^{-2\lambda_{n-2}}(R + p^{\lambda_{n-1}}\mathcal{O}_K)$$

is a co-cyclic subgroup of index $p^{\lambda_{n-1}-2\lambda_{n-2}}$. Furthermore, if R is a subring, then R' is a subring. We say that R is *rounded* to R'.

We can also count the number of subgroups that get rounded to a particular co-cyclic subgroup.

More generally, this rounding can be done towards rings of type

$$(0, \dots 0, \underbrace{e, \dots, e}_{l})$$

with $1 \leq l \leq n-1$. Using ring theory, we can give also estimates for the number of these types of rings as well (like in the co-cyclic case). Using all these roundings we get the upper bound $F(5) \leq \frac{20}{11}$.

References

[1] J. Nakagawa, *Orders of a quartic field*, Memoirs of the American Mathematical Society **583** (1996).

Third moment of certain exponential sums over finite fields

Florent Jouve

To deal with the problem of evaluating an exponential sum over finite fields, it often turns out that trying to see that exponential sum as a particular element of a whole family can be a good strategy. One of the most striking instances illustrating that fact (and which was historically of great importance) is the problem of evaluating the seemingly simple "exponential sum"

$$\sum_{x \in U(\mathbf{F}_q)} 1\,,$$

where $\mathbf{F}_q$ is the finite field with cardinality q and U is an algebraic variety defined over $\mathbf{F}_q$.

Classically, we introduce then the Zeta function of $U/\mathbf{F}_q$:

$$Z(U/\mathbf{F}_q; T) = \exp\Big(\sum_{n \geq 1} |U(\mathbf{F}_{q^n})| \frac{T^n}{n}\Big)\,,$$

where $|U(\mathbf{F}_{q^n})|$ is the number of $\mathbf{F}_{q^n}$-rational points on U. The zeta function of $U/\mathbf{F}_q$ is defined by considering the family of rational points $U(\mathbf{F}_{q^n})$ *for all* $n \geq 1$; and that function is known (thanks to a celebrated theorem of Dwork) to be rational. From that rationality we deduce easily a very interesting a priori form for the quantity $|U(\mathbf{F}_q|$.

In this talk I want to give two examples of how applying that general philosophy can really provide explicit formulæ. From now on, we fix a prime number p different

from 2 and 3 and $q = p^r$ for an integer $r \geq 1$. Let φ denote a non-trivial additive character of $\mathbf{F}_q$.

In our first example, we consider, for $a \in \mathbf{F}_q$, the sum

$$S(a^4, a^2; q) = \sum_{x \in \mathbf{F}_q} \varphi(a^4 x^3 + a^2 x)\,,$$

and its third moment (introduced by Birch for modularity issues (see [1]))

$$B_3(q) = \sum_{a \in \mathbf{F}_q} S(a^4, a^2; q)^3\,.$$

Our aim is to compute explicitely $B_3(q)$ (we easily notice that the computation of the moments of lower order are straightforward). Orthogonality relations yield

$$B_3(q) = q|S(\mathbf{F}_q)|\,,$$

where S is the affine surface given by $x^3 + y^3 + z^3 + x + y + z = 0$. Its projective compactification, defined by

$$\widetilde{S}:\ x^3 + y^3 + z^3 + w^2(x + y + z) = 0\,, \tag{1}$$

is a smooth projective cubic surface. Moreover it is obvious that

$$|S(\mathbf{F}_q)| = |\widetilde{S}(\mathbf{F}_q)| - |E(\mathbf{F}_q)|\,,$$

where E is the elliptic curve given by the homogeneous equation $x^3 + y^3 + z^3 = 0$. It is well known (see [6]) that for such a curve we have $|E(\mathbf{F}_q)| = q + 1 - \lambda_1^r - \lambda_2^r$ where $\lambda_1\lambda_2 = p$ and, either $p \equiv 1 \pmod 3$, in which case $\lambda_1 + \lambda_2 = A_p$ as soon as we write the decomposition $4p = A_p^2 + 27B^2$ with $A_p \equiv -1 \pmod 3$, or $\lambda_1 + \lambda_2 = 0$.

We are now reduced to determining the quantity $|\widetilde{S}(\mathbf{F}_q)|$. From the general theory of 2-dimensional smooth projective varieties over finite fields (see for instance [4]), we have the a priori form of the Zeta function of $\widetilde{S}$ over $\mathbf{F}_q$

$$Z(\widetilde{S}/\mathbf{F}_q; T) = \frac{P_1(T)P_3(T)}{(1 - T)(1 - q^2T)P_2(T)}\,,$$

where $P_i(T) \in \mathbf{Z}[T]$ for $1 \leq i \in\leq 3$.

Moreover (see [5]), as $\widetilde{S}$ is a smooth cubic surface, we know that $P_1(T) = P_3(T) = 1$ and that $\deg P_2 = 7$. Hence we deduce the two equivalent formulæ

$$Z(\widetilde{S}/\mathbf{F}_q; T)^{-1} = (1 - T)(1 - q^2T)P_2(T) \text{ i.e. } |\widetilde{S}(\mathbf{F}_q)| = q^2 + 1 + q\sum_{i=1}^{7} \eta_i\,,$$

where the η_i are algebraic numbers. We need to compute $\sum_{i=1}^{7} \eta_i$. We exploit a theorem of Swinnerton-Dyer (see [9]) asserting that such a sum is entirely determined by the action of the Frobenius morphism (raising coordinates to their q-th power) on the set of 27 lines contained in $\widetilde{S}$. To do so, we need to find equations for those lines. First we notice that, looking carefully at (1), we can easily obtain some of those lines e.g.

$$\mathcal{D}_z:\ (t : -t : 0 : w)\,.$$

Starting with these few lines, we can apply the method of hyperplane sections described in [8] to obtain all of the others. Finally, computing the orbits of those 27 lines under the action of Frobenius, we obtain, thanks to the theorem of Swinnerton-Dyer [9] and with λ_1 and λ_2 as above,

- if $p \equiv 1 \pmod 3$ and if we let $\epsilon = 1$ if 4 is a cube modulo p and $\epsilon = -1$ otherwise,

$$B_3(q) = q(q^2 + (2 + 2\chi_q(-1) + \zeta_6^{\delta r} + \bar{\zeta_6}^{\delta r})q - \lambda_1^r - \lambda_2^r)\,,$$

  where χ_q is the Legendre character of $\mathbf{F}_q$, ζ_6 et $\bar{\zeta_6}$ are the primitive 6-th roots of 1 in $\mathbf{C}$ and $\delta = (3 - \chi_p(-1)(2\epsilon + 1))/2$.
- if $p \equiv 2 \pmod 3$, then

$$B_3(q) = q(q^2 + (3 + (-1)^r + 2\chi_q(-1))q - \lambda_1^r - \lambda_2^r)\,.$$

Our second example involves the well known Kloosterman sums and their third moment restricted to the squares of $\mathbf{F}_q$, respectively defined by

$$K(\lambda; q) = \sum_{x \in \mathbf{F}_q^\times} \varphi(x + \lambda x^{-1}) \text{ and } \sigma_3(q) = \sum_{\lambda \in \mathbf{F}_q} K(\lambda^2; q)^3\,.$$

D. H. and E. Lehmer introduced and computed $\sigma_3(q)$ (in the case $r = 1$) in [7]. We emphasize here the geometric interpretation we give for such sums. First, orthogonality relations yield

$$\sigma_3(q) = -(q-1)^3 + q|S_0(\mathbf{F}_q)| - 1\,,$$

where S_0 is the surface defined by $x + +y + z + x^{-1} + y^{-1} + z^{-1} = 0$. Elementary transformations on that equation enable us to deduce that there is an explicit link between $|S_0(\mathbf{F}_q)|$ and $|S(\mathbf{F}_q)|$ where

$$S\,: s^2 = xy(x + y + 1)(xy + y + x)\,.$$

To compute the (minimal) smooth projective model $\widetilde{S}$ of S, we need to construct the smooth projective model of $\mathbf{P}^2$ ramified over the singular sextic curve C : $XYZ(X + Y + Z)(XY + YZ + XZ) = 0$. As C only has double points and triple points as singularities, we deduce (see [2, page 189]) that $\widetilde{S}$ is a $K3$ surface so that, as in the previous example, we have

$$Z(\widetilde{S}/\mathbf{F}_q; T)^{-1} = (1 - T)(1 - q^2T)P_2(T)\,,$$

but with this time $\deg P_2 = 22$. To determine P_2, more geometric arguments are needed (following [3] in which $\widetilde{S}$ was introduced for the first time, we can exploit the fact that $\widetilde{S}$ can be realized as an elliptic surface over $\mathbf{F}_q$). Among those arguments, we emphasize that over any extension of $\mathbf{F}_q$ containing a primitive cube root of 1, the surface $\widetilde{S}$ is isomorphic to the Kummer surface $\mathrm{Km}(E \times E)$ (see [2]) where E is the elliptic curve with Weierstrass model $y^2 = x^3 + 1$. That explains the geometric origin of the decompsition $p = a^2 + 3b^2$ (when $p \equiv 1 \pmod 6$) in [7]. Finally obtaining an explicit form for $Z(\widetilde{S}/\mathbf{F}_q; T)$, we deduce the formula

$$\sigma_3(q) = \epsilon^r q^2 + q(2q\chi_q(-1) + \chi_q(-1)(\lambda_1^r + \lambda_2^r) + 2)$$

where

- if $p \equiv -1 \bmod 6$, $\epsilon = -1$ and $\lambda_1 = p$, $\lambda_2 = -p$,
- if $p \equiv 1 \bmod 6$, $\epsilon = 1$ and λ_1 and λ_2 are the reciprocal roots of the polynomial $p^2T^2 - (4a^2 - 2p)T + 1$.

References

[1] A. O. L. Atkin, *Note on a paper of Birch*, J. London Math. Soc. **44** (1969).
[2] W. Barth, C. Peters and A. van de Ven, *Compact complex surfaces*, Springer, (1984).
[3] F. Beukers and J. Stienstra, *On the Picard-Fuchs equation and the formal Brauer group of certain elliptic K3-surfaces*, Math. Ann. **271** (1985), 269–304.
[4] P. Deligne, *Cohomologie étale, SGA* $4\frac{1}{2}$, LNM **569** Springer Verlag (1977).
[5] J. W. Hoffman and S. H. Weintraub, *The Siegel modular variety of degree two and level three*, Trans. Amer. Math. Soc. **353** number 8 (2000), 3267–3305 .
[6] K. Ireland and M. Rosen, *A classical introduction to modern number theory*, Second Edition, GTM **84**, Springer-Verlag (1990).
[7] D. H. and E. Lehmer, *On the cubes of Kloosterman sums*, Acta Arith. **6** (1960), 15–22.
[8] T. W. Sederberg, *Techniques for cubic algebraic surfaces*, IEEE Comp. Graph. and Appl. (September 1990).
[9] H. P. F. Swinnerton-Dyer, *The zeta function of a cubic surface over a finite field*, Proc. Camb. Phil. Soc. **63** (1967), 55–71.

Ranks of elliptic curves over function fields

Alan G. B. Lauder

There is a widely held belief that one half of all elliptic curves have infinitely many rational points, but all experimental data that has been collected so far suggests that the fraction is actually two thirds. The final purpose of my lecture is to present experimental evidence supporting the widely held belief. The evidence given relates to elliptic curves over function fields rather than number fields. It was gathered using a new method for computing zeta functions of varieties over finite fields.

Primitive root densities for rank 1 tori

Willem Jan Palenstijn
(joint work with Bart de Smit)

Artin's primitive root conjecture gives for a non-zero integer x an expression for the density of primes q for which x is a primitive root modulo q. We consider an analogue for rank one tori, extending work of Yen-Mei Chen [2] and Peter Stevenhagen, Hendrik Lenstra and Pieter Moree [3].

Let K be a number field, T a rank one torus over K and A a non-torsion point of $T(K)$. For a prime number p define $B_p = \langle T(K), \sqrt[p]{A}, Z_p \rangle \subset T(\bar{K})$, where Z_p is a non-trivial p-torsion point of $T(\bar{K})$. Furthermore, define B_∞ as the group generated by all B_p.

Theorem. *With notation as above,* $\mathrm{Gal}(K(B_\infty)/K)$ *is an open, normal subgroup of* $\mathrm{Aut}_{T(K)}(B_\infty)$ *with a finite, abelian cokernel, which we call the* entanglement group.

Write E for this cokernel, $E^\vee$ for its dual, and $A_p = \mathrm{Aut}_{T(K)}(B_p)$. Then, we have the following conjecture.

Artin's primitive root conjecture for rank one tori. *The density of primes* $\mathbf{q}$ *of* K *for which* $T(\mathbf{F}_\mathbf{q})$ *is generated by* $\bar{A}$ *is*

$$C_{T,A} \cdot \prod_{p \text{ prime}} \Big(1 - \frac{1}{\#A_p}\Big),$$

with $C_{T,A} \in \mathbf{Q}$ *given by*

$$C_{T,A} = \sum_{\chi \in E^\vee} \prod_{\substack{p \text{ prime} \\ \chi(A_p) \neq 1}} \frac{-1}{\#A_p - 1}.$$

Hooley proved this conjecture in 1967 for $K = \mathbf{Q}$ and $T = \mathbf{G}_\mathrm{m}$ assuming the Generalized Riemann Hypothesis. A generalization of Hooley's argument by Cooke and Weinberger [1] allows us to prove the above conjecture when assuming the GRH.

References

[1] G. Cooke and P.J. Weinberger, *On the construction of division chains in algebraic number rings, with applications to* SL_2, Comm. Algebra **3** (1975), 481–524.

[2] Y.-M. Chen, *On primitive roots of one-dimensional tori*, J. Number Theory **93** (2002), no. 1, 23–33.

[3] P. Stevenhagen, *The correction factor in Artin's primitive root conjecture*, J. Théor. Nombres Bordeaux **15** no. 1 (2003), 383–391.

The Manin conjectures for K3 surfaces

Ronald van Luijk

This is a talk about work in progress. Little is known about the arithmetic of K3 surfaces. It is for instance not known if there exists a K3 surface X over a number field k such that the set $X(k)$ of k-rational points on X is neither empty, nor dense. Examples of K3 surfaces are smooth quartic surfaces in $\mathbb{P}^3$, which we focus on in this talk. We will look at the growth of the number of rational points of bounded height on such surfaces. Despite our lack of knowledge, it seems that this growth is very well behaved. Consider a surface X over a number field k, choose a height H corresponding to some ample divisor, and for each open subset $U \subset X$ set

$$N_U(B) = \#\{x \in U(k) \ : \ H(x) \leq B\}.$$

The Manin conjectures state that if the anticanonical divisor on X is ample, and H is the height associated to it, then there exists a field extension l/k, a nonempty open subset $U \subset X_L$ and a constant C, such that

$$N_U(B) \sim CB(\log B)^{b-1},$$

where b equals the rank of $\operatorname{Pic} X_L$. A priori, there are not many reasons why similar asymptotics would exist for K3 surfaces. If they do, one knows they are of the form $\mathcal{O}(B^\varepsilon)$ for any $\varepsilon > 0$. In this talk we present evidence that if X is a K3 surface, then we have

$$N_U(B) \sim C(\log B)^b,$$

with U and b as before. There will, however, be some restrictions. If X admits an elliptic fibration, for instance, then we can not expect these asymptotics to hold, as infinitely many fibers may each contain more rational points than the asymptotics predict for a dense open subset. We therefore only look at surfaces with small Picard number b of which we know that they do not admit an elliptic fibration.

We also compute a (relatively naive) constant $\tilde{C}$, based on local contributions. In the Fano case described above, where the anticanonical divisor is ample, Emmanuel Peyre has given a conjectured constant that differs from $\tilde{C}$ by a rational number of small height.

In all (so far, a little more than a handful) examples where we computed all rational points up to a reasonable height we see that N_U indeed appears to converge to $C(\log B)^b$ for some constant C that differs from the a priori computed naive constant $\tilde{C}$ by a rational factor of height at most 3. In the future, after more explicit computations, we intend to phrase a precise conjecture.

A non-local obstruction for equation of the type $z^n = F(x, y)$

Denis Simon

Our starting point is the following result, which is a classical application of composition of quadratic forms.

Theorem 1 (see [1]). *Let (a, b, c) be three coprime integers such that $D = b^2 - 4ac$ is not a square. Let $d \geqslant 1$ be an integer. Then the equation $ax^2 + bxy + cy^2 = y^d$ has a primitive solution (x and z are coprime integers) with y coprime to $2D$ if and only if the class of the form $ax^2 + bxy + cy^2$ is a d–th power in the class group $Cl(D)$.*

My goal is to generalize the "⇒" part of this for binary forms of degree $n > 2$.

Let $F(x, z) = a_0x^n + a_1x^{n-1}z + \cdots + a_nz^n$ be a homogeneous binary form with integral coefficients. Assume that F is irreducible over $\mathbb{Q}$ and primitive (the a_i are coprime).

Following [2], we define an order $\mathbb{Z}_F$ in the splitting field K of F. The discriminant of this order is exactly the discriminant of F. This order $\mathbb{Z}_F$ is contained in

the maximal order $\mathbb{Z}_K$ of K and in general $Ind(F) = [\mathbb{Z}_K : \mathbb{Z}_F]$ is a positive integer that can be > 1. We also define an element $cl(F)$ in the class group $Cl(\mathbb{Z}_F)$.

We prove the following:

Theorem 2. *Let F be as above and $d \geqslant 1$. If the equation $F(x, z) = y^d$ has a primitive solution (x and z are coprime integers) such that y is coprime to $Ind(F)$, then $cl(F)$ is a d–th power in the class group $Cl(\mathbb{Z}_F)$.*

In the following tables, we record some forms F of degree 4 and 3, such that $Ind(F) = 1$. For these forms, we indicate their discriminant and the type of the class group $Cl(\mathbb{Z}_F)$. We also record the value of $cl(F)$ in this group. Finally, the last column indicates a list of values of d for which our theorem proves that their exists no primitive solution to $y^d = F(x, z)$.

Disc(F)	F	$Cl(\mathbb{Z}_F)$	$cl(F)$	d
2448	$2x^4 + 2x^3 - 5x^2 - 2x + 5$	$\mathbb{Z}/2\mathbb{Z}$	(1)	2
13785	$4x^4 - 3x^3 + 14x^2 - 5x + 11$	$\mathbb{Z}/3\mathbb{Z}$	(1)	3
14504	$4x^4 - 5x^3 - 6x^2 + 5x + 4$	$\mathbb{Z}/4\mathbb{Z}$	(2)	4
13396	$2x^4 - 2x^3 + 6x^2 - 3x + 5$	$\mathbb{Z}/5\mathbb{Z}$	(3)	5
43245	$2x^4 - 3x^3 + x^2 + 3x + 2$	$\mathbb{Z}/6\mathbb{Z}$	(1)	2, 3
25205	$2x^4 - x^3 + 5x^2 + x + 2$	$\mathbb{Z}/7\mathbb{Z}$	(1)	7
438445	$3x^4 - 2x^3 + 8x^2 + x + 4$	$\mathbb{Z}/8\mathbb{Z}$	(4)	8
235901	$2x^4 - x^3 - 7x^2 + x + 10$	$\mathbb{Z}/9\mathbb{Z}$	(3)	9
77648	$2x^4 - 6x^3 + 5x^2 + 10x + 3$	$\mathbb{Z}/10\mathbb{Z}$	(7)	2, 5
330781	$3x^4 - 4x^3 + 4x^2 + 5x + 2$	$\mathbb{Z}/11\mathbb{Z}$	(1)	11
122728	$4x^4 + 3x^3 - 6x^2 - 3x + 4$	$\mathbb{Z}/12\mathbb{Z}$	(10)	3, 4
146548	$2x^4 - 2x^3 + 8x^2 - x + 3$	$\mathbb{Z}/13\mathbb{Z}$	(12)	13
141681	$3x^4 - 4x^3 + 11x^2 - 5x + 7$	$\mathbb{Z}/14\mathbb{Z}$	(3)	2, 7

Disc(F)	F	$Cl(\mathbb{Z}_F)$	$cl(F)$	d
-648	$2x^3 + 3x^2 + 2$	$\mathbb{Z}/3\mathbb{Z}$	(1)	3
-1879	$2x^3 + x^2 - x + 4$	$\mathbb{Z}/4\mathbb{Z}$	(2)	4
-1572	$2x^3 + 2x^2 + x + 4$	$\mathbb{Z}/5\mathbb{Z}$	(2)	5
-2856	$2x^3 + 2x^2 + 5x - 3$	$\mathbb{Z}/7\mathbb{Z}$	(3)	7
-18628	$4x^3 - 9x^2 + 4x + 7$	$\mathbb{Z}/8\mathbb{Z}$	(4)	8
-22443	$8x^3 + 5x^2 - 3x + 3$	$\mathbb{Z}/9\mathbb{Z}$	(3)	9
-12244	$3x^3 - 4x^2 + 7x + 4$	$\mathbb{Z}/11\mathbb{Z}$	(1)	11
-19919	$2x^3 - 5x^2 + 7x + 10$	$\mathbb{Z}/12\mathbb{Z}$	(2)	3, 4
-9064	$5x^3 - 4x^2 - 5x + 6$	$\mathbb{Z}/13\mathbb{Z}$	(9)	13

Looking at this table for $n = 3$, we observe that there is no example with $d = 2$. As suggested by this observation, we prove

Proposition 3. *Let F be irreducible and primitive of degree n. Assume that $Ind(F) = 1$. Let $\mathfrak{d}$ denote the different of $\mathbb{Z}_F$. Then we have $[\mathfrak{d}] = cl(F)^{n-2}$ in $Cl(\mathbb{Z}_F)$.*

By Hecke's theorem, we know that $[\mathfrak{d}]$ is always a square in $Cl(\mathbb{Z}_K)$ ($= Cl(\mathbb{Z}_F)$ in this case). When the degree n is odd, this proves that $cl(F)$ is also a square, hence proving the observation. When the degree n is even, this construction provides an explicit square root of $[\mathfrak{d}]$.

In particular, when $d = 2$ and $n = 3$, we want to represent squares by cubic forms. After some amount of computations, we ask the following question:

Question 4. *Let F be any primitive binary cubic form. Is it true that F always primitively represent a square?*

I do not know any counterexample to this. In the talk, I state a partial answer to the question by showing

Proposition 5. *Let F be any primitive binary cubic form. There exist coprime integers x and z, and an integer y such that*

- *either $F(x, z) = y^2$*
- *or $F(x, z) = 2y^2$.*

References

[1] J.W.S. Cassels: *Rational Quadratic Forms*, L.M.S. Monographs, Academic Press (1978).
[2] D. Simon: *La classe invariante d'une forme binaire*, Comptes Rendus Mathématiques, **336**, Issue 1, (2003) 7–10.

Parity conjecture for elliptic curves

Tim Dokchitser
(joint work with Vladimir Dokchitser)

Suppose E is an elliptic curve (or a principally polarised abelian variety) defined over a number field K. An identity between the L-functions $L(E/K_i, s)$ for extensions K_i of K induces a conjectural relation between the Birch–Swinnerton-Dyer quotients. Using the BSD-invariance under Weil restriction and under isogenies, it is not hard to prove that these relations actually hold, assuming only finiteness of the Tate-Shafarevich group Ш. In fact, without assuming that Ш is finite, it is possible to give unconditional statements about Selmer groups as well.

I discussed a method to interpret these relations and use them to deduce special cases of various parity conjectures:

"Weak" Parity Conjecture. Assuming Ш is finite,

$$(-1)^{\mathrm{rk}(E/K)} = w(E/K).$$

"Strong" Parity Conjecture. For every prime p,

$$(-1)^{\mathrm{rk}_p(E/K)} = w(E/K). \qquad (\Longrightarrow \text{ Weak P.C.})$$

"Even stronger" Parity Conjecture.

$$(-1)^{\mathrm{rk}(E/K)} = w(E/K). \qquad (\Longrightarrow \text{ Strong P.C.})$$

As an example, suppose for simplicity that E/K is semistable, and suppose $\mathrm{Gal}(F/K) \cong S_3$, with subfields as follows:

$$\left.\begin{array}{ccc} & F & \\ C_3 & & C_2 \\ & M & \\ & K & \end{array}\right) \begin{array}{l} \\ \\ M' \\ \\ \end{array} \quad G = S_3.$$

Then

$$L(E/F,s)L(E/K,s)^2 = L(E/M,s)L(E/M',s)^2.$$

If $Ш(E/F)$ is finite, the relation between BSD-quotients reduces to

$$\frac{R_{E/F}\, {R_{E/K}}^2}{R_{E/M}\, {R_{E/M'}}^2} \quad \equiv \quad \frac{C_{E/F}\, {C_{E/K}}^2}{C_{E/M}\, {C_{E/M'}}^2} \qquad \mathrm{mod}\ \mathbb{Q}^{*2}$$

where R is the regulator and C the product of local Tamagawa numbers. It is then not hard to see that

$$\mathrm{LHS} \equiv 3^{\mathrm{rk}(E/K)+\mathrm{rk}(E/M)+\mathrm{rk}(E/M')} \mod 2.$$

and a purely local computation shows

$$\mathrm{ord}_3(\mathrm{RHS})\ \text{even} \iff w(E/K)w(E/M)w(E/M') = 1,$$

a special case of the parity conjecture.

Our main application is the following result, completing earlier work of various authors, notably Birch-Stephens, Greenberg-Guo, Nekovář and Kim.

Theorem 1. Strong Parity Conjecture holds for all $E/\mathbb{Q}$.

Corollary. Either $(-1)^{\mathrm{rk}(E/\mathbb{Q})} = w(E/\mathbb{Q})$ or $\mathbb{Q}/\mathbb{Z} \subset Ш(E/\mathbb{Q})$.

The second application is that modulo some restrictions at 2 and 3, for elliptic curves over general number fields parity follows from finiteness of Ш:

Theorem 2. Weak Parity Conjecture is true for all E/K that are semistable at $v|6$ and not supersingular at $v|2$.

References

[1] T. Dokchitser, V. Dokchitser, On the Birch–Swinnerton-Dyer quotients modulo squares, 2006, arxiv: math.NT/0610290.

2^n-descent on elliptic curves

Sir Peter Swinnerton-Dyer

Let E be an elliptic curve over a number field k. To implement a 2-descent on E it is necessary to write it in the form $Y^2 = (X - \alpha_1)(X - \alpha_2)(X - \alpha_3)$ by means of a field extension; the 2-coverings which are locally soluble have the form

$$Z_i^2 = \lambda_i(X - \alpha_i) \quad \text{for } i = 1, 2, 3 \qquad \text{and} \quad Z_1 Z_2 Z_3 = Y, \tag{1}$$

where $\lambda_1\lambda_2\lambda_3 = 1$ and some obvious conjugacy conditions hold. For this to be everywhere locally soluble, the λ_i must be units at all good primes.

It is usually said that a 4-descent involves working in the field of definition of a 4-division point; but Cassels in 1999 showed how to do this while working inside the $k(\alpha_i)$. In this talk I show how to generalize this to 2^n-descent for all n.

Let C be a curve of genus 1 with Jacobian E, defined over k and everywhere locally soluble. Then there exist functions f_i in $k(\alpha_i)(C)$ and F in $k(C)$ such that the 2-coverings of C have the form

$$Z_i^2 = \lambda_i f_i \quad \text{for } i = 1, 2, 3 \qquad \text{and} \quad Z_1 Z_2 Z_3 = F, \tag{2}$$

where $\lambda_1\lambda_2\lambda_3 = 1$. Moreover *either* there are no triples $(\lambda_1, \lambda_2, \lambda_3)$ for which (2) is everywhere locally soluble *or* the triples for which (2) is everywhere locally soluble are just those for which (1) is everywhere locally soluble. Moreover one can test which of these happens without constructing the f_i.

The proof of the existence of such f_i depends on the local-to-global theorem for Severi–Brauer varieties; and the implementation of the process depends on being able to find points on a Severi–Brauer variety defined over $k(\alpha_i)$. This appears to be a difficult problem.

LLL and numerical analysis

Damien Stehlé

Lattice reduction is a central tool in many areas in mathematics and computer science. Some of its applications require very fast algorithms and implementations. To achieve this efficiency goal, floating-point arithmetic is used within these algorithms, most often heuristically, to compute Gram-Schmidt orthogonalisations.

In this talk, I show how to use classical results from numerical analysis to guarantee the correctness of these algorithms relying on floating-point arithmetic. I survey the 2005 L^2 algorithm of Nguyen and Stehlé [2] that uses floating-point approximations within the famous LLL algorithm [1], as well as ongoing research on the numerical stability of the QR-factorisation and the use of floating-point arithmetic in the computation of Hermite-Korkine-Zolotarev reduced bases.

References

[1] A.K. Lenstra, H.W. Lenstra Jr and L. Lovász, *Factoring polynomials with rational coefficients*, Mathematische Annalen **261** (4), 515–534, 1982.

[2] P.Q. Nguyen and D. Stehlé, *Floating-point LLL revisited*, Proceedings of Eurocrypt 2005, volume 3494 of Lecture Notes in Computer Science, 215–233. Springer Verlag, 2005.

A tighter analysis of Kannan's enumeration algorithm

Guillaume Hanrot

(joint work with Damien Stehlé)

Let $L = (b_1, \ldots, b_d)$ be a lattice in $\mathbb{R}^n$. Though efficient methods exist to find short nonzero vectors in L, it is required in some applications to find one shortest nonzero vector in L. A theorem by Ajtai asserts that it is a difficult problem, more precisely an NP-hard problem under randomized reductions.

A simple algorithm due to Kannan [5] (also known as Fincke-Pohst's algorithm [2]) exists for this task: namely, enumerate the $x \in L$ within the ball $B := \{\|x\| \leq \|b_1\|\}$. The way of analyzing this enumeration is by relating lattice points in L to integer points within the ellipsoid $E := \{(y_i) \in \mathbb{Z}^d / \sum_{i=1}^d y_i^2 \|b_i^*\|^2 \leq 4\|b_1\|^2\}$, where (b_i^*) is the Gram-Schmidt orthogonalization of the basis b_i. The complexity of this enumeration highly depends on the quality/reduction strength of the input basis.

We shall say that $(b_1, \ldots, b_d)$ is an HKZ-reduced basis if b_1 is a shortest vector of L, and if $\mathrm{proj}_{<b_1>^\perp}(b_2, \ldots, b_d)$ is an HKZ-reduced basis of $\mathrm{proj}_{<b_1>^\perp}(L)$. The basis is quasi-HKZ reduced iff. $\mathrm{proj}_{<b_1>^\perp}(b_2, \ldots, b_d)$ is HKZ-reduced and $\|b_2^*\| \geq \|b_1\|/2$.

Previous analyses [4, 5] estimate this number of points by the volume of the outer parallelepiped, which is

$$\prod_{i=1}^{d} \frac{\|b_1\|}{\|b_i^*\|} \leq 2^d d^{d/2},$$

the latter inequality being valid if the basis is quasi-HKZ reduced. Our analysis improves on this approximation by proving that the right order of magnitude is closer to the volume of the inner parallelepiped. Indeed, we have [3]:

Theorem 1. *The number of integer points in E is bounded by*

$$2^{O(d)} \prod_{i=1}^{d} \max\left(1, \frac{\|b_1\|}{\sqrt{d}\|b_i^*\|}\right).$$

From this formula, we see that the largest the $\|b_i^*\|$ the best. This means that in order for this algorithm to be practical, one first has to perform a large precomputation on the basis in order to reduce it strongly. In his original paper, Kannan already performs simultaneously Hermite-Korkine-Zolotareff (HKZ)-reduction on the basis while computing the shortest vector. This means that we can assume

that the basis we are working with is already quasi-HKZ-reduced. In that setting, we have [3]:

Theorem 2. *Assume that tbe basis b_i is quasi HKZ-reduced. Then, for all $I \subset \{1, \dots, d\}$, one has*

$$\prod_{i \in I} \|b_i^*\| \geq \|b_1\|^{|I|} d^{-|I|(1+\log \frac{d}{|I|})}.$$

As a conclusion, Kannan's algorithm checks at most $d^{d/2e+o(d)}$ candidate points in the worst case. Work in progress based on ideas from [1] suggests that our analysis is sharp.

References

[1] M. Ajtai, *The worst-case behavior of Schnorr's algorithm approximating the shortest nonzero vector in a lattice*, Proceedings of the 35th Symposium on the Theory of Computing (STOC 2003), 396–406.

[2] U. Fincke, M. Pohst, *A procedure for determining algebraic integers of given norm*, Proceedings of EUROCAL, Springer-Verlag Lecture Notes in Computer Science **162** (1983), 194–202.

[3] G. Hanrot, D. Stehlé, *Improved Analysis of Kannan's Shortest Lattice Vector Algorithm*, Proceedings of Crypto'2007, to appear.

[4] B. Helfrich, *Algorithms to Construct Minkowski Reduced and Hermite Reduced Lattice Bases*, Theoret. Comput. Sci. **41** (1985), 125–139.

[5] R. Kannan, *Improved algorithms for integer programming and related lattice problems*, Proceedings of the 15th Symposium on the Theory of Computing (STOC 1983), 99–108.

Computations of values of p-adic L-functions of real quadratic fields

Xavier-François Roblot

Let E be a real quadratic field and, for $\mathfrak{f}$ a modulus of E, denote by $\mathrm{Cl}_{\mathfrak{f}}(E)$ the ray class group of E modulo $\mathfrak{f}$. Let χ be an abelian character of $\mathrm{Cl}_{\mathfrak{f}}(E)$ with values in $\bar{\mathbb{Q}}$. We fix an embedding of $\bar{\mathbb{Q}}$ into $\mathbb{C}_p$, therefore χ can also be seen as having values in $\mathbb{C}_p$. The L-function of χ is defined by

$$L(s, \chi) = \prod_{\mathfrak{q} \nmid \mathfrak{f}_0} \left(1 - \chi(\mathfrak{q}) \mathcal{N}\mathfrak{q}^{-s}\right)^{-1} \quad \text{for } \Re(s) > 1,$$

where $\mathfrak{q}$ runs through the prime ideals of E not dividing the finite part $\mathfrak{f}_0$ of the modulus $\mathfrak{f}$. It is well-known that this function can be extended to the whole complex plane to an analytic function if the character χ is non trivial, otherwise it is a meromorphic function with a simple pole at $s = 1$.

Deligne-Ribet [5], Cassou-Noguès [3] and Barsky [1] proved independently that there exists a continuous p-adic function $L_p(s, \chi)$, the so-called p-adic L-function of χ, that interpolates $L(s, \chi)$ in the following sense: let ϕ denote the Euler totient

function and set $q = 4$ if $p = 2$ and $q = p$ otherwise, then for all integers $k \leq 0$ such that $k \equiv 1 \pmod{\phi(q)}$, we have

$$L_p(k,\chi) = \prod_{\mathfrak{p}|p} \left(1 - \chi(\mathfrak{p})\mathcal{N}\mathfrak{p}^{-k}\right) L(k,\chi). \tag{1}$$

We use a reinterpretation of the construction of the p-adic L-functions of Cassou-Noguès and Barsky using p-adic measures, due to Katz [6], see also [4] and [2], to explicitely compute values of these functions.

Let $\mathfrak{c}$ be a prime ideal of E, of residual degree 1, relatively prime with $\mathcal{D}$, the codifferent of E, and such that $\chi(\mathfrak{c}) \neq 1$. Let $\nu \in (\mathfrak{c}\mathcal{D})^{-1}$ be such that

$$\mathrm{Tr}(\nu)\mathbb{Z} = \mathrm{Tr}((\mathfrak{c}\mathcal{D})^{-1}).$$

The function $\alpha \mapsto \xi(\alpha) = \exp(2i\pi\mathrm{Tr}(\nu\alpha))$ is an additive character of order $c = \mathcal{N}\mathfrak{c}$ on $\mathbb{Z}_E$, the ring of integers of E, such that

$$\sum_{i=0}^{c-1} \xi(\alpha)^i = \begin{cases} 0 & \text{if } \alpha \notin \mathfrak{c}, \\ c & \text{otherwise.} \end{cases}$$

For an integral ideal $\mathfrak{a}$, relatively prime to $\mathfrak{f}$, we define the twisted partial zeta functions

$$Z(s,\mathfrak{a},i) = \sum_{\alpha \in R(\mathfrak{a})} \xi(\alpha)^i \mathcal{N}\alpha^{-s} \quad \text{for } \Re(s) > 1,$$

where $R(\mathfrak{a})$ is a set of representatives of $\{\alpha \in \mathbb{Z}_E^+ \cap \mathfrak{a} \text{ with } (\alpha, p) = 1\}$ under the action of $U_{\mathfrak{f}}(E)^+ = \{u \in U(E) \cap \mathbb{Z}_E^+ \text{ and } u \equiv 1 \pmod{\mathfrak{f}}\}$, and $\mathbb{Z}_E^+$ is the subset of totally positive elements in $\mathbb{Z}_E$. These functions admit analytic continuation to $\mathbb{C}$ and are linked to L-functions in the following way

$$L(s,\chi) = \left(c^{1-s}\chi(\mathfrak{c}) - 1\right)^{-1} \prod_{\mathfrak{p}|p} \left(1 - \chi(\mathfrak{p})\mathcal{N}\mathfrak{p}^{-s}\right)^{-1} \sum_{\mathfrak{a}} \mathcal{N}\mathfrak{a}^s \sum_{i=1}^{c-1} Z(s,\mathfrak{a},i) \tag{2}$$

where $\mathfrak{a}$ runs through a set of integral ideals representing all the classes of $\mathrm{Cl}_{\mathfrak{f}}(E)$.

Using methods originating from the works of Shintani [7], one can construct power series $F_{\mathfrak{a},i}(T_1,T_2) \in \bar{\mathbb{Q}}[T_1,T_2]$ such that

$$\left[\Delta^{-k} F_{\mathfrak{a},i}(T_1,T_2)\right]_{T_1=T_2=0} = Z(k,\mathfrak{a},i) \quad \text{for all } k \in \mathbb{Z}_{\leq 0} \tag{3}$$

where Δ is the operator

$$\Delta = (1+T_1)(1+T_2)\frac{\partial^2}{\partial T_1 \partial T_2}.$$

Then the theory of p-adic integration enables one to associate to a power series $F(T_1,T_2)$ with bounded coefficients in $\mathbb{C}_p$ a measure μ_F over $\mathbb{Z}_p^2$ such that

$$\left[\Delta^t F(T_1,T_2)\right]_{T_1=T_2=0} = \int (x_1x_2)^t \, d\mu_F(x_1,x_2) \quad \text{for all } t \in \mathbb{Z}_{\geq 0}. \tag{4}$$

Using the embedding of $\bar{\mathbb{Q}}$ into $\mathbb{C}_p$ that we fixed in the introduction, we can regard $F_{\mathfrak{a},i}$ as having coefficients in $\mathbb{C}_p$. Unfortunately, unless p is split in E, this power

series does not have bounded coefficients. To fix this, we let $\gamma \in \mathbb{Z}_E$ be such that $\mathbb{Z}_E = \mathbb{Z} + \gamma\mathbb{Z}$ and we consider the change of variables

$$T_1 \leftarrow (1+T_1)(1+T_2) - 1, \quad T_2 \leftarrow (1+T_1)^{\gamma}(1+T_2)^{\gamma'} - 1 \tag{5}$$

where γ' is the conjugate of γ. This change of variables is inversible and applying its inverse to $F_{\mathfrak{a},i}$, we obtain a power series $G_{\mathfrak{a},i}$ now having bounded coefficients. Putting together (3), (4) and (5), and letting $\mu_{\mathfrak{a},i}$ be the measure associated to $G_{\mathfrak{a},i}$, we get the following

$$\int \mathcal{N}(x_1 + x_2\gamma)^{-k}\, d\mu_{\mathfrak{a},i}(x_1, x_2) = Z(k, \mathfrak{a}, i) \quad \text{for all } k \leq 0,$$

where $\mathcal{N}$ denotes the absolute value of the norm from E to $\mathbb{Q}$.

It is not difficult to build p-adic continuous functions ψ_s, with $s \in \mathbb{Z}_p$, such that $s \mapsto \psi_s$ is a continuous map, the functions ψ_s's are zero on $p\mathbb{Z}_p$ and satisfy the following interpolation property

$$\psi_t(x) = x^t \quad \text{for all } t \in \mathbb{Z}_{\geq 0} \text{ such that } t \equiv -1 \pmod{\phi(q)}.$$

The p-adic twisted partial zeta function is defined by

$$Z_p(s, \mathfrak{a}, i) = \int \psi_{-s}\big(\mathcal{N}(x_1 + x_2\gamma)\big)\, d\mu_{\mathfrak{a},i}(x_1, x_2).$$

It is a continuous function on $\mathbb{Z}_p$, and if we use the p-adic equivalent of (2), which means basically replacing the function $x \mapsto x^{-s}$ by the function ψ_{-s}, to define the p-adic L-function $L_p(s, \chi)$, we get a continuous function on $\mathbb{Z}_p$ (or $\mathbb{Z}_p \setminus \{1\}$ if χ is trivial) satisfying (1).

We now briefly explain how to compute approximate values of $Z_p(s, \mathfrak{a}, i)$. Write

$$G_{\mathfrak{a},i}(T_1, T_2) = \sum_{n_1, n_2 \geq 0} g(\mathfrak{a}, i)_{n_1,n_2} T_1^{n_1} T_2^{n_2}$$

and, for $s \in \mathbb{Z}_p$, let

$$\psi_s\big(\mathcal{N}(x_1 + x_2\gamma)\big) = \sum_{n_1, n_2 \geq 0} a(s)_{n_1,n_2} \binom{x_1}{n_1} \binom{x_2}{n_2}$$

be the Mahler expansion of this function, so that $a(s)_{n_1,n_2} \to 0$ when $n_1 + n_2 \to \infty$. The coefficients $a(s)_{n_1,n_2}$ can easily be computed from the values at positive integers of the function $(x_1, x_2) \mapsto \psi_s\big(\mathcal{N}(x_1 + x_2\gamma)\big)$. We then have

$$Z_p(s, \mathfrak{a}, i) = \int \psi_{-s}\big(\mathcal{N}(x_1 + x_2\gamma)\big)\, d\mu_{\mathfrak{a},i}(x_1, x_2) = \sum_{n_1, n_2 \geq 0} g(\mathfrak{a}, i)_{n_1,n_2} a(-s)_{n_1,n_2}.$$

By truncating this sum to a finite sum by discarding terms such that $n_1 + n_2 \geq N$, for a suitable large enough positive integer N, one gets a good approximation of the value of $Z_p(s, \mathfrak{a}, i)$.

References

[1] D. Barsky, *Fonctions zêta p-adiques d'une classe de rayon des corps de nombres totalement réels*, Groupe d'étude d'analyse ultramétrique 1977–78. Errata, idem 1978–79.

[2] D. Barsky, *Sur la nullité du mu-invariant d'Iwasawa des corps totalement réels*, available on arXiv: math/0405487v1.

[3] Pi. Cassou-Noguès, *Valeurs aux entiers négatifs des fonctions zêta et fonctions zêta p-adiques*, Invent. Math. **51** (1979), 29–59.

[4] P. Colmez, *Résidu en $s = 1$ des fonctions zêta p-adiques*, Invent. Math. **91** (1988), 371–389.

[5] P. Deligne and K. Ribet, *Values of abelian L-functions at negative integers over totally real fields*, Invent. Math. **59** (1980), 227–286.

[6] N. Katz, *Another look at p-adic L-functions for totally real number fields*, Math. Ann. **255** (1981), 33–43.

[7] T. Shintani, *On evaluation of zeta functions of totally real algebraic number fields*, Journal Fac. Sci. Univ. Tokyo, Sec. IA, **23**, (1976), 393–417.

Quadratic twists of rank 1

Christophe Delaunay

(joint work with Xavier-François Roblot)

The main goal is to study the behavior of the regulators of elliptic curves with rank 1 belonging to a family of quadratic twists of a fixed elliptic curve E defined over $\mathbb{Q}$. The methods coming from random matrix matrix theory as developed in [K-S], [CKRS], [CFKRS] etc. allow us to derive precise conjectures for the moments of those regulators. We hope those moments can help in the predictions for the number of extra-rank (i.e. number of odd quadratic twists[1] E_d having a Mordell-Weil rank greater than 3). We have developed in [De-Ro] an efficient Heegner-point construction method to compute explicitly the regulator (and the order of the Tate-Shafarevich group) of elliptic curves with rank 1 in a quadratic twist family. The numerical data (of the families of odd twists of the curves $11a1$, $14a1$, $15a1$ and $17a1$) are in close agreement with our predictions.

Suppose that E has conductor N and that for all primes p dividing N we have fixed a sign w_p such that $\prod_{p|N} w_p = w(E)$ where $w(E)$ is the sign of the functional equation of E. Let

$$\mathcal{F} = \left\{ d < 0,\ \text{fundamental discriminant with } \left(\frac{d}{p}\right) = w_p \text{ for all } p \mid N \right\}$$

and

$$\mathcal{F}(T) = \left\{ d \in \mathcal{F},\ |d| < T \right\}.$$

Then, our family of quadratic twists is $(E_d)_{d\in\mathcal{F}}$. The choices of the w_p imply that $w(E_d) = -1$ for all $d \in \mathcal{F}$. If $L'(E_d, 1) \neq 0$ then the elliptic curve E_d has rank 1 and hence the Mordeil-Weil group $E_d(\mathbb{Q})$ is generated by one generator G_d up to torsion and the regulator $R(E_d)$ of E_d is then the canonical height $\hat{h}(G_d)$

[1] An odd (resp. even) quadratic twist is a quadratic twist of E such that the sign of the functional equation of its L-function is -1 (resp. $+1$). By the Birch and Swinnerton-Dyer conjecture, that we assume here, this is the same as to say that its Mordell-Weil rank is odd (resp. even)

of G_d. Our heuristic gives an asymptotic formula for the moment of order k (with $0 < k < 1$) of $R(E_d)$; more precisely it states that for $0 < k < 1$ we should have

$$\frac{1}{|\mathcal{F}(T)|} \sum_{\substack{d \in \mathcal{F}(T) \\ L'(E_d,1) \neq 0}} R(E_d)^k \sim A_E(k) T^{k/2} \log(T)^{b_E(k)} \text{ as } T \to \infty$$

where the constant $b_E(k)$ is explicit and mainly depends on the field of definition of the 2-torsion points of E.

From a numerical and experimental point of view, the situation of odd quadratic twists differs from the even-rank one. Indeed, in the latter case, we consider a family $(E_d)_d$ of even quadratic twists of a fixed elliptic curve. For each curve E_d one has to compute the special value $L(E_d, 1)$ of its L-function and to determine if it is zero or not. If $L(E_d, 1) = 0$ the curve E_d contributes to the extra-rank otherwise the curves has rank 0 and the regulator is simply 1; the Birch and Swinnerton-Dyer conjecture allows then to deduce $|Ш(E_d)|$ from $L(E_d, 1)$. The computation of $L(E_d, 1)$ is done via a Waldspurger's like formula which roughly speaking states that $L(E_d, 1)$ is up to some fudge factor the square of the $|d|$-th coefficient of a weight $3/2$ modular form often given by a linear combination of theta series. It follows that huge computations are possible (see for example [Rub], [Qua] etc.). The numerical data are in close agreement with the well-known conjectures of [CKRS] about extra-vanishing (coming from the models of random matrix theory) or on the behavior of the Tate-Shafarevich groups $Ш(E_d)$ of E_d (see [Qua], [De1]).

In the rank 1 case, the numerical point of view appears to be more complicated. In that case, we first have to compute the value of the derivative $L'(E_d, 1)$ for each curves E_d in our family of odd quadratic twists. Nevertheless, on the one hand there is no Waldspurger's formula to compute it directly, and on the other hand, even if we had computed it, it is just possible to deduce from it (via the Birch and Swinnerton-Dyer conjecture and if it is nonzero) the values of the product $R(E_d)|Ш(E_d)|$. Then, we also need to evaluate at least one of the two members of the previous product.[2] The only (know) efficient possibility is to write down a generator G_d of $E_d(\mathbb{Q})$ and to compute $R(E_d) = \hat{h}(G_d)$ where $\hat{h}$ is the canonical height of E_d.

In our method, we first adapt directly the Heegner-point construction and replacing Waldspurger's formula by Gross and Zagier's one. This allows us to compute directly the regulator $R(E_d)$ *and at the same time* the order of the Tate-Shafarevich group $|Ш(E_d)|$ (assuming the Birch and Swinnerton-Dyer conjecture).

[2]For some families of elliptic curves $(F_j)_j$, there can exist a generic point in the Mordel-Weil group $F_j(\mathbb{Q})$ and then one can separate the terms in the product of the Birch and Swinnerton-Dyer formula and a direct investigation is then possible [De-Du]. Nevertheless, such families, for which we know in advance the regulator, are very special and in particular are not quadratic families (however we must precise that it is possible to get sometime a generic point for some very specific and tiny sub-family of quadratic twist).

References

[CKRS] J. B. Conrey, J. P. Keating, M. O. Rubinstein and N. C. Snaith, *On the frequency of vanishing of quadratic twists of modular L-functions*, Number theory for the millennium, I (Urbana, IL, 2000), 301–315, A K Peters, Natick, MA, 2002.

[CFKRS] J. B. Conrey, D. W. Farmer J. P. Keating, M. O. Rubinstein and N. C. Snaith, *Integral moments of L-functions*, Proc. London Math. Soc. (3) **91** (2005), no. 1, 33–104.

[CRSW] J. B. Conrey, M. O. Rubinstein, N. C. Snaith and M. Watkins, *Discretisation for odd quadratic twists*, in Rank of elliptic curves and random matrix theory, ed. J. B. Conrey, D. W. Farmer, F. Mezzadri and N. C. Snaith, London Mathematical Society, Lecture notes series **341**, 201–214.

[De1] C. Delaunay, *Heuristics on class groups and on Tate-Shafarevitch groups*, in Rank of elliptic curves and random matrix theory, ed. J. B. Conrey, D. W. Farmer, F. Mezzadri and N. C. Snaith, London Mathematical Society, Lecture notes series **341**, 323–340.

[De2] C. Delaunay, *Moments of the Orders of Tate-Shafarevich groups*, International Journal of Number Theory, **1** (2005), no. 2, 243–264.

[De-Du] C. Delaunay and S. Duquesne, *Numerical Investigations Related to the Derivatives of the L-series of Certain Elliptic Curves*, Exp. Math. **12** (2003), no. 3, 311–317.

[De-Ro] C. Delaunay and X.-F. Roblot, *Regulators of rank 1 quadratic twists*, preprint available on arXiv (:0707.0772).

[K-S] J. P. Keating and N. C. Snaith, *Random matrix theory and L-functions at $s = 1/2$*, Comm. Math. Phys. **214** (2000), 91–110.

[Qua] P. Quattrini, *On the distribution of analytic $\sqrt{|Ш|}$ values on quadratic twists of elliptic curves*, Experiment. Math. **15** (2006), no. 3, 355–365.

[Rub] M. Rubinstein, *Numerical data*, available at `http://www.math.uwaterloo.ca/~mrubinst`

[Sna] N. Snaith, *Derivatives of random matrix characteristic polynomials with applications to elliptic curves*, J. Phys. A 38 (2005), **48**, 10345–10360.

Finding rational points on elliptic curves using 6-descent and 12-descent

Tom A. Fisher

Let E be an elliptic curve over $\mathbb{Q}$. An n-descent calculation on E provides us with n-covering curves $\pi_\alpha : C_\alpha \to E$ for α running over a finite indexing set A, with the property that

$$\bigcup_{\alpha \in A} \pi_\alpha(C_\alpha(\mathbb{Q})) = E(\mathbb{Q}).$$

The usual choice of indexing set A is the n-Selmer group $S^{(n)}(E/\mathbb{Q})$ which sits in a short exact sequence

$$0 \to E(\mathbb{Q})/nE(\mathbb{Q}) \xrightarrow{\delta} S^{(n)}(E/\mathbb{Q}) \to Ш(E/\mathbb{Q})[n] \to 0.$$

Given $\alpha \in S^{(n)}(E/\mathbb{Q})$ there are two possibilities: either $\pi_\alpha(C_\alpha(\mathbb{Q}))$ is a coset of $nE(\mathbb{Q})$ in $E(\mathbb{Q})$, in which case α is the image of this coset by δ, or $C_\alpha(\mathbb{Q})$ is empty, in which case α maps to a non-zero element of the Tate-Shafarevich group $Ш(E/\mathbb{Q})$.

It has long be known that n-descent can help in the search for generators of the Mordell-Weil group $E(\mathbb{Q})$. Indeed the theory of heights (see for example [7]) suggests that if we write our n-coverings as curves of degree n, with small

coefficients, then a point of (logarithmic) height h on $E(\mathbb{Q})$ should come from a point of height approximately $h/(2n)$ on $C_\alpha(\mathbb{Q})$ for suitable α. This is not a precise statement (the height is only bounded up to the addition of a constant whose behaviour with respect to n is unknown) but the idea seems to work well in practice.

We would therefore like to perform n-descent calculations for n as large as possible. Until recently n-descent has only been practical for general elliptic curves in the case $n = 2$. (By general we mean that no assumptions are made on the Galois module structure of $E[n]$.) Methods for 4-descent and 8-descent have been developed in the PhD theses of Siksek [9], Womack [13] and Stamminger [10]. Joint work of the author with Cremona, O'Neil, Simon and Stoll [3] has now made 3-descent practical, and in a few preliminary examples also 5-descent. The algorithms for 2-descent, 3-descent and 4-descent, for elliptic curves over $\mathbb{Q}$, have been contributed to the computer algebra system MAGMA [8]. The n-covering curves are returned as (equations for) curves of degree n in $\mathbb{P}^{n-1}$ (respectively as $y^2 =$ quartic, if $n = 2$).

Given coprime integers m and n we would like to combine an m-covering and an n-covering to produce an mn-covering. We have found a practical method for doing this, based on representations of the Heisenberg group, that works whenever each of m and n is plus or minus a square modulo the other. This includes the case where m and n are consecutive. More precisely, in that case, we specify an embedding of E in $\mathbb{P}(\mathrm{Mat}_{n,n+1})$, as a curve of degree $n(n+1)$, in such a way that when E acts on itself by translation, the n-torsion points act as left multiplication by $n \times n$ matrices, and the $(n+1)$-torsion points act as right multiplication by $(n+1) \times (n+1)$ matrices. We can then twist E by a pair of cocycles taking values in $E[n]$ and $E[n+1]$ to obtain the required $n(n+1)$-covering $C_{n(n+1)}$ as a curve in $\mathbb{P}(\mathrm{Mat}_{n,n+1})$. Conveniently, the covering map $C_{n(n+1)} \to C_{n+1}$ is defined by taking $n \times n$ minors. Our implementations of 6-descent and 12-descent (*i.e.* the cases $n = 2, 3$) are further simplified by using formulae coming from the invariant theory of binary quartics and ternary cubics.

If an n-covering $\pi : C \to E$ is to be useful in the search for rational points on E, not only must we find explicit equations for $C \subset \mathbb{P}^{n-1}$, but we must also make a change of co-ordinates on $\mathbb{P}^{n-1}$ so that these equations have reasonably small coefficients. The task naturally falls into two parts which, following terminology introduced by Cremona, we call minimisation and reduction.

Minimisation is the task of removing as many prime factors as possible from a suitably defined discriminant. The most familiar example is that of minimising a Weierstrass equation. By reduction we mean the use of unimodular transformations to further decrease the size of the coefficients. The basic example is reduction of binary quadratic forms, or more generally lattice reduction. Thus minimisation is concerned with the finite places, and reduction with the infinite places. The need to perform reduction is our main reason for working over $\mathbb{Q}$ (instead of a more general number field).

The minimisation and reduction of 2-coverings is described in [1], [2], and [5]. Generalisations to 3-coverings and 4-coverings are given in [4] and [13]. These algorithms are included as part of the MAGMA implementations of 2-descent, 3-descent and 4-descent. Hence in our implementations of 6-descent and 12-descent we start with an n-covering and an $(n+1)$-covering both of which are already minimised and reduced. So it not unreasonable to hope that the $n(n+1)$-covering we compute will automatically be minimised and reduced. Numerical examples suggest that this is true for reduction, but not for minimisation. For minimisation we currently use a limited number of ad hoc tricks, based on the behaviour of the defining equations when reduced mod p. Although these methods work reasonably well in practice, there remains considerable room for both theoretical and practical improvements.

Once we have minimised and reduced our equations for C we must then search for rational points on C. We use the p-adic point searching method due independently to Elkies and Heath-Brown, as implemented by Watkins in the MAGMA function `PointSearch`. Descriptions may be found in [12] and [13, §2.9]. (Elkies' original paper [6] only considers real approximations.) The method first chooses an auxiliary prime p, whose size depends on the height bound set for the search. The points on the reduction of C mod p are then enumerated, and for each such point P_0 a lattice method variant of Hensel's lemma is used to search for rational points on C with reduction P_0. A variant of the method uses two primes. The method works particularly well for curves of high codimension as considered here.

Using 12-descent, we now expect to be able to find rational points on an elliptic curve over $\mathbb{Q}$ up to logarithmic height 600 (provided the discriminant of the original elliptic curve is not too large, for practical reasons). The main bottleneck comes in the 3-descent, where we must compute the class group and units of each number field generated by the co-ordinates of a 3-torsion point of E. (There is usually just one such field, and it has degree 8.) Fortunately, since our final answer comes in the form of a rational point, there is no need to perform these intermediate calculations rigorously.

As an application we show that every elliptic curve (of prime conductor) in the Stein-Watkins database [11] has rank at least as large as predicted by the conjecture of Birch and Swinnerton-Dyer. Prior to our involvement this had been reduced by Cremona and Watkins to a list of 35 elliptic curves of analytic rank 2, for which one generator of small height (less than 34) was known, but a second generator of large height (greater than 220) remained to be found. In each case we were able to find the second generator using either 6-descent or 12-descent. For example the second generator on the elliptic curve

$$y^2 + y = x^3 - 237882589x - 1412186639384$$

has height 642.626.

Acknowledgments

I would like to thank Steve Donnelly for sharing his initial thoughts on 6-descent, and Mark Watkins for suggesting suitable test data.

References

[1] B.J. Birch and H.P.F. Swinnerton-Dyer, Notes on elliptic curves I. *J. Reine Angew. Math.* **212** (1963), 7–25.

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

[3] J.E. Cremona, T.A. Fisher, C. O'Neil, D. Simon and M. Stoll, *Explicit n-descent on elliptic curves, I Algebra*, to appear *J. Reine Angew. Math.*, *II Geometry*, submitted for publication, *III Algorithms*, in preparation.

[4] J.E. Cremona, T.A. Fisher and M. Stoll, *Minimisation and reduction for 3- and 4-coverings of elliptic curves*, in preparation.

[5] J.E. Cremona and M. Stoll, Minimal models for 2-coverings of elliptic curves, *LMS J. Comput. Math.* **5** (2002), 220–243 (electronic).

[6] N.D. Elkies, Rational points near curves and small nonzero $|x^3 - y^2|$ via lattice reduction, *Algorithmic number theory* (Leiden, 2000), 33–63, Lecture Notes in Comput. Sci., 1838, Springer, Berlin, 2000.

[7] M. Hindry and J.H. Silverman, *Diophantine geometry*, Graduate Texts in Mathematics 201, Springer-Verlag, New York, 2000.

[8] MAGMA is described in W. Bosma, J. Cannon and C. Playoust, The Magma algebra system I: The user language, *J. Symbolic Comput.* 24, 235–265 (1997). The Magma home page is at `http://magma.maths.usyd.edu.au/magma/`

[9] S. Siksek, *Descent on curve of genus* 1, PhD thesis, University of Exeter, 1995.

[10] S. Stamminger, *Explicit 8-descent on elliptic curves*, PhD thesis, International University Bremen, 2005.

[11] W.A. Stein and M. Watkins, A database of elliptic curves—first report, *Algorithmic number theory* (Sydney, 2002), 267–275, Lecture Notes in Comput. Sci., 2369, Springer, Berlin, 2002.

[12] M. Watkins, *Searching for points p-adically*, notes available from `http://www.maths.bris.ac.uk/~mamjw/papers/`

[13] T. Womack, *Explicit descent on elliptic curves*, PhD thesis, University of Nottingham, 2003.

Algorithmic representation of a curve and its Picard group

Kamal Khuri-Makdisi

Abstract: Let C be a smooth projective algebraic curve over a field k. I describe how one can represent C without explicit equations, by using instead the "values" of global sections of line bundles on C at sufficiently many points of C. This representation of C leads to fast algorithms for divisors and divisor classes on C, as well as to interesting approaches to finding explicit models for modular and Shimura curves.

1. Statement on Research

I am currently pursuing various theoretical and algorithmic questions related to modular curves, with the goal of eventually generalizing the results to Shimura curves associated to an indefinite quaternion algebra over $\mathbf{Q}$. The ideas grew out of earlier work of mine [KM04a,KM04b] on algorithms for divisors and divisor classes on algebraic curves. I have been developing systematic and general methods to find and work with equations of modular curves. These methods should extend to the case of Shimura curves, and should give a good computational handle on the

Jacobians (more precisely, the degree zero Picard groups) of modular and Shimura curves and their endomorphisms by Hecke operators T_p for small p.

I specifically wish to compute with exact elements of number fields, not with complex approximations. In the setting of Shimura curves, this means that I would need to get a handle on a number of automorphic forms on the quaternion algebra, together with an interpretation of their "values" in terms of the abelian surfaces with quaternionic multiplication parametrized by the Shimura curve. I call such an interpretation "moduli-friendly." In the setting of modular curves, a simple example of this is the two Eisenstein series of weights 4 and 6 on the full modular group $SL(2, \mathbf{Z})$, whose "values" at a point on the modular curve $X(1)$ corresponding to an elliptic curve $E : y^2 = x^3 + ax + b$ are essentially the values of the coefficients a and b. (Here the idea is to parametrize not just elliptic curves, but rather pairs (E, ω) with a choice of global differential ω on E; this pins down the values of a and b, and allows us to genuinely talk of evaluating an elliptic modular form at such an object.) I can give a moduli-friendly interpretation of all holomorphic Eisenstein series on the congruence subgroup $\Gamma(\ell)$. Moreover, I conjecture that all modular forms of weight 3 and above on $\Gamma(\ell)$ are polynomials in the weight 1 Eisenstein series, which have a particularly direct moduli interpretation. (The corresponding statement about weight 1 Eisenstein series on the subgroup $\Gamma_1(\ell)$ is a result of Borisov and Gunnells [BG01b, BG03]. The above conjecture thus states that their result extends to $\Gamma(\ell)$.)

Theorem 1. *Assume that the above conjecture holds. Given just* one *curve E_0 without complex multiplication, defined (say) over $\mathbf{Q}$, then using all the coordinates of the torsion points in $E_0[\ell]$ allows us to obtain equations for the modular curve $X(\ell)$ over the field $\mathbf{Q}(E_0[\ell])$. Hence these equations describe* all *modular curves with level ℓ structure. With some more work we can reduce the field of definition to the cyclotomic field $\mathbf{Q}(\mu_\ell)$, and perhaps even to $\mathbf{Q}$. For the modular curve $X_1(\ell)$, we obtain an analogous result unconditionally.*

The above method of obtaining models for modular curves is well suited for working with their Jacobians. More generally, the following is my philosophy for describing curves and for working with their Jacobians, which grew out of my work in [KM04a, KM04b]. Let C be a smooth projective curve of moderately large genus g and gonality over a perfect field k.

Philosophy 2. (1) *The best way to represent the curve C is to choose a line bundle $\mathcal{L}$ on C with $\deg \mathcal{L} = N + g \geq 2g + 2$ but $\deg \mathcal{L} = O(g)$ nonetheless. Then we must arrange to know explicitly the spaces $V = H^0(C, \mathcal{L})$ and $V' = H^0(C, \mathcal{L}^{\otimes 2})$, as well as the multiplication map $\mu : V \otimes V \to V'$. (For modular curves, V will be a space of modular forms $\mathcal{M}_\kappa(\Gamma)$ of given weight κ, while $V' = \mathcal{M}_{2\kappa}(\Gamma)$.)*

(2) *The most efficient way to keep track of the multiplication μ is to represent elements of V and V' by their values at sufficiently many points of C. (In the setting of modular curves, this means knowing the values of elements of $\mathcal{M}_\kappa(\Gamma)$ and $\mathcal{M}_{2\kappa}(\Gamma)$, evaluated in a moduli-friendly way at sufficiently many tuples (E, ω, α), where α is a level structure for Γ.)*

Statement (1) above is equivalent to knowing equations for C, since the complete linear series corresponding to the $(N+1)$-dimensional space $V = H^0(C, \mathcal{L})$ gives a projective embedding of C into $\mathbf{P}^N$, where the homogeneous ideal $I_C \subset k[T_0, \ldots, T_N]$ describing the image of C is generated by its elements of degree 2 due to the assumption on $\deg \mathcal{L}$; these elements of degree 2 are implicit in our knowledge of the map μ. Statement (2) above says that rather than storing a multiplication table, we are better off representing elements of V and V' by their values at points of C. (In Section 2 of [KM04b], this is the difference between using "Representation A" and "Representation B"; in Section 5 of that article, we describe how to convert a curve from Representation A into Representation B.) To be able to talk about the value of a section at various points, we need to choose (at least implicitly) a trivialization of $\mathcal{L}$ near each such point. This removes the need for knowing the multiplication table of μ, since we merely need to multiply values; on the other hand, we must take enough points to be able to identify elements of V and V' by their values at those points. A conservative choice is to evaluate at $1 + 2\deg \mathcal{L}$ points; alternatively, we can take $\dim V'$ points in general position on the curve.

Using the above model of C, we can represent certain divisors by subspaces of V: let D be a k-rational effective divisor with $\deg D \leq \deg \mathcal{L} - 2g$. Then we represent D by the k-rational subspace $W_D \subset V$ consisting of the linear functions that vanish on D (to the correct multiplicity), and we similarly define $W'_D \subset V'$, by

$$W_D := H^0(C, \mathcal{L}(-D)) \subset V, \qquad W'_D := H^0(C, \mathcal{L}^{\otimes 2}(-D)) \subset V'.$$

I used the above representation in [KM04b] to give the asymptotically fastest known algorithms for the group law in the Picard group of a general curve:

Theorem 3. *Let C be any curve of genus g, represented as above. Then there exist efficient randomized algorithms for the group operations (i.e., addition, inversion, subtraction, equality testing, and membership testing) in the Picard group $(\mathrm{Pic}^0 C)(k)$. Each such group operation takes an expected $O(g^{2.376})$ field operations in k, and the result is guaranteed to be correct.*

The above complexity of $O(g^{2.376})$ involves fast linear algebra; if we use Gaussian elimination instead, the complexity rises to $O(g^{3+\epsilon})$. The previous record for general curves had been a complexity of $O(g^4)$, by Florian Hess [Hes99]; his algorithms however attain a faster complexity ($O(g^2)$) than mine for special curves such as hyperelliptic or trigonal curves, whose gonality is small compared to their genus. On the other hand, my general algorithms are quite simple to implement, involving nothing more than linear algebra on subspaces of V and V', and the multiplication μ. Even for special curves of small genus, my approach is algorithmically efficient: in recent work [ASKM06], Fatima Abu Salem and I obtained a 20% speedup over previous methods [BEFG04, FOR04] for computations in the Picard group of $C_{3,4}$ curves, which have genus 3.

References

[ASKM06] Fatima Abu Salem and Kamal Khuri-Makdisi, *Fast Jacobian group operations for $C_{3,4}$ curves over a large finite field*, `http://arxiv.org/abs/math.NT/0610121` preprint, 2006.

[BEFG04] Abdolali Basiri, Andreas Enge, Jean-Charles Faugère, and Nicolas Gürel, *Implementing the arithmetic of $C_{3,4}$ curves*, Algorithmic number theory, Lecture Notes in Comput. Sci., vol. 3076, Springer, Berlin, 2004, pp. 87–101. MR 2137346 (2006a:14101)

[BG01b] ———, *Toric varieties and modular forms*, Invent. Math. **144** (2001), no. 2, 297–325. MR 1826373 (2002g:11053)

[BG03] ———, *Toric modular forms of higher weight*, J. Reine Angew. Math. **560** (2003), 43–64. MR 1992801 (2004f:11037)

[FOR04] Stéphane Flon, Roger Oyono, and Christophe Ritzenthaler, *Fast addition on non-hyperelliptic genus 3 curves*, `http://www.exp-math.uni-essen.de/~oyono/Quartic.html` preprint, 2004.

[Hes99] Florian Hess, *Zur Divisorenklassengruppenberechnung in globalen Funktionenkörpern*, Ph.D. thesis, Technische Universität Berlin, 1999, may be downloaded from the web at the URL `http://www.math.tu-berlin.de/~kant/publications.html`.

[KM04a] ———, *Linear algebra algorithms for divisors on an algebraic curve*, Math. Comp. **73** (2004), no. 245, 333–357 (electronic), `math.NT/0105182`. MR 2034126 (2005a:14081)

[KM04b] ———, *Asymptotically fast group operations on Jacobians of general curves*, `http://arxiv.org/abs/math.NT/0409209`, to appear in Mathematics of Computation.

Reporter: Peter Bruin

Participants

Prof. Dr. Karim Belabas
Laboratoire d'Algorithmique
Arithmetique
Universite Bordeaux I
351 cours de la Liberation
F-33405 Talence Cedex

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

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

Dr. Andrew Booker
School of Mathemtics
University of Bristol
University Walk, Clifton
GB-Bristol , BS8 1TW

Dr. Wieb Bosma
IMAPP
Radboud Universiteit Nijmegen
Toernooiveld 1
NL-6525 ED Nijmegen

Jos Brakenhoff
Mathematisch Instituut
Universiteit Leiden
Postbus 9512
NL-2300 RA Leiden

Peter Bruin
Mathematisch Instituut
Universiteit Leiden
Postbus 9512
NL-2300 RA Leiden

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

Prof. Dr. Marie-Line Chabanol
Laboratoire A2X
UFR de Math. et Informatique
Universite Bordeaux I
351, cours de la Liberation
F-33405 Talence Cedex

Prof. Dr. Henri Cohen
Laboratoire A2X
UFR de Math. et Informatique
Universite Bordeaux I
351, cours de la Liberation
F-33405 Talence Cedex

Prof. Dr. Jean-Marc Couveignes
Departement de Mathematiques et
Informatique; UFR S.E.S.
Universite Toulouse II
5, Allee Antonio Machado
F-31058 Toulouse Cedex 9

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

Dr. Christophe Delaunay
Institut Camille Jordan
Universite Claude Bernard Lyon 1
43 blvd. du 11 novembre 1918
F-69622 Villeurbanne Cedex

Prof. Dr. Jean-Marc Deshouillers
Laboratoire A2X
UFR de Math. et Informatique
Universite Bordeaux I
351, cours de la Liberation
F-33405 Talence Cedex

Prof. Dr. Tim Dokchitser
Dept. of Pure Mathematics and
Mathematical Statistics
University of Cambridge
Wilberforce Road
GB-Cambridge CB3 OWB

Prof. Dr. Noam D. Elkies
Dept. of Mathematics
Harvard University
Science Center
One Oxford Street
Cambridge MA 02138-2901
USA

Prof. Dr. Jordan S. Ellenberg
Department of Mathematics
University of Wisconsin-Madison
480 Lincoln Drive
Madison , WI 53706-1388
USA

Dr. Tom A. Fisher
Centre for Mathematical Sciences
University of Cambridge
Wilberforce Road
GB-Cambridge CB3 OWB

Prof. Dr. Eugene Victor Flynn
New College
University of Oxford
GB-Oxford OX1 3BN

Dr. Herbert Gangl
Dept. of Mathematical Sciences
Durham University
Science Laboratories
South Road
GB-Durham , DH1 3LE

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

Dr. Guillaume Hanrot
INRIA NANCY / LORIA
Boite Postale 239
F-54506 Vandoeuvre les Nancy Cedex

Wei Ho
Department of Mathematics
Princeton University
Fine Hall
Washington Road
Princeton , NJ 08544
USA

Florent Jouve
Mathematiques et Informatique
Universite Bordeaux I
351, cours de la Liberation
F-33405 Talence Cedex

Prof. Dr. Kamal Khuri-Makdisi
Department of Mathematics
American University of Beirut
Riad El-Solh
P.O.Box 11-0236
Beirut 1107 2020
LEBANON

Prof. Dr. Jürgen Klüners
Mathematisches Institut
Heinrich-Heine-Universität
Gebäude 25.22
Universitätsstraße 1
40225 Düsseldorf

Dr. David R. Kohel
School of Mathematics & Statistics
The University of Sydney
Sydney NSW 2006
AUSTRALIA

Dr. Alan G. B. Lauder
Mathematical Institute
Oxford University
24-29 St. Giles
GB-Oxford OX1 3LB

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

Dr. Ronald van Luijk
Department of Mathematics
Simon Fraser University
8888 University Dr.
Burnaby , B.C. V5A 1S6
CANADA

Prof. Dr. Jean-Francois Mestre
U. F. R. de Mathematiques
Case 7012
Universite Paris VII
2, Place Jussieu
F-75251 Paris Cedex 05

Pascal Molin
Departement de Mathematiques et
Applications
Ecole Normale Superieure
45, rue d'Ulm
F-75005 Paris Cedex

Anna Morra
Laboratoire A2X
UFR de Math. et Informatique
Universite Bordeaux I
351, cours de la Liberation
F-33405 Talence Cedex

Willem Jan Palenstijn
Mathematisch Instituut
Universiteit Leiden
Postbus 9512
NL-2300 RA Leiden

Prof. Dr. Michael E. Pohst
Fakultät II -Institut f. Mathematik
Technische Universität Berlin
Sekr. MA 8-1
Straße des 17. Juni 136
10623 Berlin

Prof. Dr. Bjorn Poonen
Department of Mathematics
University of California
Berkeley , CA 94720-3840
USA

Dr. Nicole Raulf
Universite de Lille I
U.F.R. de Mathematiques Pures
et Appliquees
F-59655 Villeneuve d' Ascq Cedex

Dr. Guillaume Ricotta
Institut de Mathematiques
Universite de Bordeaux I
351 Cours de la Liberation
F-33405 Talence

Dr. Xavier-Francois Roblot
Institut Camille Jordan
Universite Claude Bernard Lyon 1
43 blvd. du 11 novembre 1918
F-69622 Villeurbanne Cedex

Prof. Dr. Samir Siksek
Department of Mathematics
University of Warwick
GB-Coventry CV4 7AL

Denis Simon
Dept. de Mathematiques et Mecanique
Universite de Caen
F-14032 Caen Cedex

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

Prof. Dr. Harold M. Stark
Dept. of Mathematics
University of California, San Diego
9500 Gilman Drive
La Jolla , CA 92093-0112
USA

Dr. Damien Stehle
ENS Lyon
LIP
46, Allee d'Italie
F-69007 Lyon Cedex

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

Prof. Dr. Michael Stoll
School of Engineering and Science
Jacobs University Bremen
Postfach 750561
28725 Bremen

Prof. Dr. Peter Swinnerton-Dyer
Dept. of Pure Mathematics and
Mathematical Statistics
University of Cambridge
Wilberforce Road
GB-Cambridge CB3 OWB

Prof. Dr. Akshay Venkatesh
Courant Institute of
Mathematical Sciences
New York University
251, Mercer Street
New York , NY 10012-1110
USA

Mark J. Watkins
School of Mathematics
Bristol University
University Walk
GB-Bristol BS8 1TW

Melanie Matchet Wood
Department of Mathematics
Princeton University
Fine Hall
Washington Road
Princeton , NJ 08544
USA

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