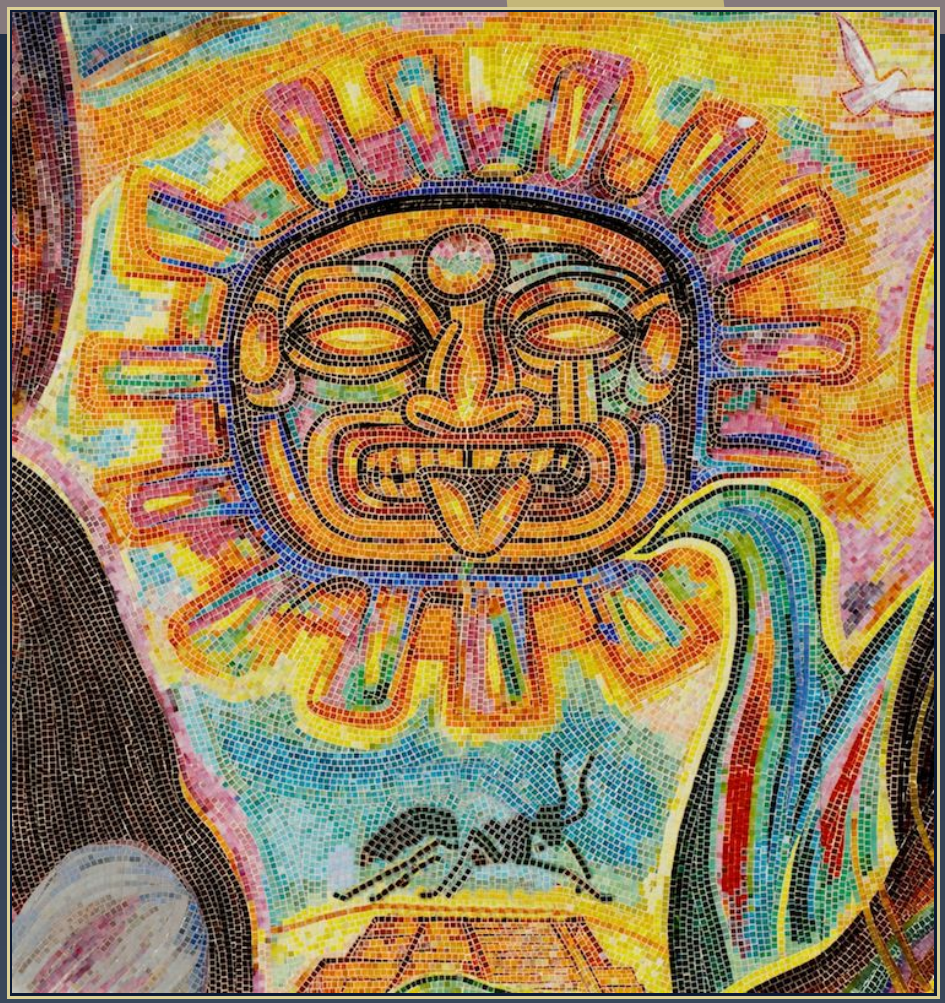
THE OPEN BOOK SERIES 1

# ANTS X
## Proceedings of the Tenth Algorithmic Number Theory Symposium

Conditionally bounding analytic ranks of elliptic curves

Jonathan W. Bober



msp

THE OPEN BOOK SERIES **1** (2013)
**Tenth Algorithmic Number Theory Symposium**
dx.doi.org/10.2140/obs.2013.1.135

msp

# Conditionally bounding analytic ranks of elliptic curves

Jonathan W. Bober

We describe a method for bounding the rank of an elliptic curve under the assumptions of the Birch and Swinnerton-Dyer conjecture and the generalized Riemann hypothesis. As an example, we compute, under these conjectures, exact upper bounds for curves which are known to have rank at least as large as 20, 21, 22, 23, and 24. For the known curve of rank at least 28, we get a bound of 30.

## 1. Introduction

Determining the rank of an elliptic curve is a difficult problem, and there is currently no known unconditional algorithm for determining the rank of a given curve. The basic method for rigorously determining the rank of a curve is to find an upper bound for the rank by computing the size of some Selmer groups and to find a lower bound for the rank by finding enough independent rational points. In theory, if one continues this process long enough, and the Shafarevich-Tate group of the curve is finite, the upper and lower bounds should eventually coincide and the rank will be determined exactly.

In practice, things are not so simple. Finding points on the curve is sometimes not too bad, but the upper bounds for the rank are more problematic. Even the computation of the 2-Selmer rank is difficult, and it becomes prohibitively time-consuming as the coefficients of the elliptic curve grow; it is easy to write down a curve for which the state-of-the-art program for computing the 2-Selmer group, John Cremona's `mwrank` [5], will effectively take "forever."

If one is willing to accept the Birch and Swinnerton-Dyer conjecture that the rank of an elliptic curve is the same as the order of vanishing of its $L$-function at the central point, then it is possible to use the $L$-function to get information

*MSC2010*: primary 11M41; secondary 14G10.
*Keywords*: elliptic curve, rank, L-function, explicit formula.

about the rank. In fact, when the order of vanishing is between 0 and 3, it can be possible to compute the $L$-function to enough precision and use some extra information about the curve to determine the analytic rank exactly, as is done in [3], for example. When the rank is larger than this, though, currently the best one can do is determine that the first $r$ derivatives of the $L$-function are very close to 0 and the $(r+1)$-st is not, which will provide a very good guess for the rank and a rigorous upper bound, assuming BSD.

This approach has its own problems, as it is much easier to write down a curve of large conductor than it is to compute the $L$-function of such a curve. For example, the known curve of rank at least 28 [8], which we will write down later, has conductor $N \approx 3.5 \times 10^{141}$, and current methods (such as those described in [19]) typically require summing on the order of $\sqrt{N}$ terms to compute the central value of the $L$-function. (It would take a computer about $10^{53}$ cpu-years just to add 1 to itself $10^{70}$ times.)

We present here a third method which is rather effective at bounding the rank, especially when the rank is large compared to the conductor, as long as one is willing to assume both the Birch and Swinnerton-Dyer conjecture and the Riemann Hypothesis for the $L$-function of the curve. This method is not completely new. It is based on Mestre's method [14] for (conditionally) bounding the rank of an elliptic curve based only on its conductor, and it was used by Fermigier [9] to study ranks of elliptic curves in certain families. However, it does not seem to have gained much traction and does not seem to have been used much, if at all, since.

The idea, in brief, is as follows. Take $f(x)$ to be a function such that $f(0) = 1$ and $f(x) \geq 0$ for all real $x$. Then, assuming the Riemann hypothesis, the sum $\sum f(\gamma)$, where $1/2 + i\gamma$ runs over the nontrivial zeros of $L(s, E)$ (counted with multiplicity), will be an upper bound for the analytic rank of $E$. Moreover, for certain choices of $f(x)$ this sum may be efficiently evaluated using the explicit formula for the $L$-function attached to $E$.

This method has recently been implemented by the author, and is available as part of William Stein's PSAGE [21] add-ons to Sage [22]. As an example of what it can do, we will examine 6 curves known to have rather large rank. We denote these curves by $E_n$, where the index $n$, taking the values $20, 21, 22, 23, 24, 28$ represents a known lower bound for the rank. We will write down these curves later (they are all taken from A. Dujella's website [6], and at the time of discovery each held the record for the curve with largest number of known independent rational points). The exact rank is not known for any of these curves. However, conditionally we may claim:

**Theorem 1.1.** *Assuming BSD and GRH, $E_n$ has rank exactly $n$ for $n = 20, 21, 22,$ 23, and 24, while $E_{28}$ has rank 28 or 30.*

**Remark 1.2.** Around the time that I was writing this paper, Andrew Booker and Jo Dwyer were able to exactly compute the rank of $E_{28}$, again assuming the Birch and Swinnerton-Dyer conjecture and the Riemann Hypothesis for $L(s, E_{28})$. They use the method described here, but by using the optimization procedure described in Section 3 of [1] they are able to select a better test function as input to the explicit formula, and they get a correspondingly better bound.

## 2. Bounding ranks

**2A.** ***The method.*** Let

$$L(s, E) = \sum_{n=1}^{\infty} \frac{a_n}{n^s} = \prod_p L_p(s, E)^{-1}$$

be the $L$-function of an elliptic curve, normalized so that the completed $L$-function $\Lambda(s, E)$ satisfies the functional equation $\Lambda(s, E) = \epsilon\Lambda(1-s, E)$, and let $c_n$ be defined by

$$-\frac{L'(s, E)}{L(s, E)} = \sum_{n=1}^{\infty} \frac{c_n}{n^s}.$$

More explicitly, if we define $\alpha(p)$ and $\beta(p)$ by

$$L_p(s, E) = (1-\alpha(p)p^{-s})(1-\beta(p)p^{-s}),$$

(note that $\alpha$ and $\beta$ are only well defined up to permutation, and that at least one of them will be 0 when $p$ is a prime of bad reduction), then

$$c_{p^m} = \big(\alpha(p)^m + \beta(p)^m\big)\log p,$$

and $c_n = 0$ when $n$ is not a prime power.

Our main tool will be the explicit formula for $L(s, E)$, which we state in a friendly form in the following lemma.

**Lemma 2.1.** *Suppose that $f(z)$ is an entire function with $f(x+iy) \ll x^{-(1+\delta)}$ for $|y| < 1+\epsilon$, for some $\epsilon > 0$, and that the Fourier transform of $f$*

$$\hat{f}(y) = \int_{-\infty}^{\infty} f(x)e^{-2\pi ixy}\mathrm{d}x$$

*exists and is such that*

$$\sum_{n=1}^{\infty} \frac{c_n}{n^{1/2}} \hat{f}\left(\frac{\log n}{2\pi}\right)$$

*converges absolutely. Then*

$$\sum_{\gamma} f(\gamma) = \hat{f}(0)\frac{\log N}{2\pi} - \hat{f}(0)\frac{\log 2\pi}{\pi} + \frac{1}{\pi}\Re\left\{\int_{-\infty}^{\infty} \frac{\Gamma'}{\Gamma}(1+it)\,f(t)\mathrm{d}t\right\} - \frac{1}{2\pi}\sum_{n=1}^{\infty}\frac{c(n)}{n^{1/2}}\left(\hat{f}\left(\frac{\log n}{2\pi}\right) + \hat{f}\left(-\frac{\log n}{2\pi}\right)\right), \quad (1)$$

*where $1/2 + i\gamma$ runs over the nontrivial zeros of $L(s, E)$, where $E$ is an elliptic curve with conductor $N$.*

*Proof.* A proof of the explicit formula in this form, or in a similar form, can be found in various sources — for example, [11, Theorem 5.12] — so we give only a brief sketch. The idea is to integrate the function

$$F(s)\frac{L'(s, E)}{L(s, E)},$$

where $F(1/2 + is) = f(s)$, on a vertical line to the right of the critical strip and, in the reverse direction, on a vertical line to the left of the critical strip. By the residue theorem, this integral will be equal to $2\pi\sum_{\gamma} f(\gamma)$. One now applies the functional equation to write the integral in the left half-plane as an integral in the right half-plane.

The sum over the Fourier coefficients of $f$ arises from shifting contours to the region of absolute convergence and using the Dirichlet series for $L'(s)/L(s)$, while the other terms arise from shifting the remaining integrals to the line $\Re(s) = 1/2$.

The conditions on $f(z)$ are exactly those needed to make sure that this process can go through without trouble. Of course, it is also important that $L(s, E)$ is entire and that it satisfies a functional equation [25; 24; 2]. □

A convenient function to use in an application of the explicit formula is

$$f(z) = f(z; \Delta) = \left(\frac{\sin(\Delta\pi z)}{\Delta\pi z}\right)^2,$$

which has the simple Fourier transform

$$\hat{f}(x; \Delta) = \left(\frac{1}{\Delta}\right)\left(1 - \left|\frac{x}{\Delta}\right|\right), \quad |x| < \Delta.$$

With this choice of $f$, Equation (1) takes the form

$$\sum_{\gamma} f(\gamma; \Delta) = \frac{\log N}{\Delta 2\pi} - \frac{\log 2\pi}{\Delta\pi} + \frac{1}{\pi}\Re\left\{\int_{-\infty}^{\infty}\frac{\Gamma'}{\Gamma}(1+it)\,f(t; \Delta)\mathrm{d}t\right\} - \frac{1}{\Delta\pi}\sum_{p \le \exp(2\pi\Delta)}\log p \sum_{k=1}^{\lfloor 2\pi\Delta/\log p\rfloor}\frac{1}{p^{k/2}}\left(\alpha(p)^k + \beta(p)^k\right)\left(1 - \frac{k\log p}{2\pi\Delta}\right). \quad (2)$$

Since $f(\gamma;\Delta)\geq 0$ as long as $\gamma$ is real, and $f(0;\Delta)=1$, Equation (2) will give an upper bound for the order of vanishing of $L(s,E)$ at $s=1/2$, as long as the Riemann Hypothesis holds for $L(s,E)$. And if $\Delta$ is not too large, we can quickly evaluate the right-hand side of Equation (2) to calculate this upper bound. It is also worth noting that, assuming RH,

$$-\lim_{\Delta\to\infty}\frac{1}{\Delta\pi}\sum_{p\leq\exp(2\pi\Delta)}\log p\sum_{k=1}^{\lfloor 2\pi\Delta/\log p\rfloor}\frac{1}{p^{k/2}}\left(\alpha(p)^k+\beta(p)^k\right)\left(1-\frac{k\log p}{2\pi\Delta}\right)$$
$$=\operatorname{ord}_{s=1/2}L(s,E)$$

so that, in principle, we should be able to get as good a bound for the rank as we like through this method. However, as the length of the prime sum grows exponentially in $\Delta$, this method quickly becomes infeasible once $\Delta$ gets a little larger than 4.

**2B.** ***Some curves.*** As an example, we examine 6 elliptic curves from Dujella's online tables. They are

$$E_{20}\colon y^2+xy=x^3-43109298076633367795836209589116 6x + 51562835553666436590356527998711769093915330881 96,$$

$$E_{21}\colon y^2+xy+y=x^3+x^2-21584377242244392201516995270215983 5x - 19474361277787151947255961435459054151501792241320535,$$

$$E_{22}\colon y^2+xy+y=x^3-94029951777639136290302312116586 4x + 10707363070719743033425295515449274534651125011362,$$

$$E_{23}\colon y^2+xy+y=x^3-19252966408674012828065964616418441723x + 32685500727716376257923347071452044295907443056345614006,$$

$$E_{24}\colon y^2+xy+y=x^3-12003982203699224530353461919116679637 4x + 50422499248491067001080179916808272675944375622291141511 6,$$

and

$$E_{28}\colon y^2+xy+y=x^3-x^2-\left(\begin{matrix}200677624155755265850332 08\times 10^{30}\\ +\ 20933854275093023031217895650 2\end{matrix}\right)x + \left(\begin{matrix}34481611795030556467032985690390720374855 94\times 10^{40}\\ +\ 43593191803612660082962919394487322434 29\end{matrix}\right).$$

Each $E_n$ has $n$ known independent rational points of infinite order, so has at least rank $n$. (See [16; 17; 10; 12; 13; 8], or [6] for quick reference.) Using

| Curve | $\log N_E$ | $\Delta$ | $\sum_\gamma f(\gamma;\Delta)$ | $\frac{\log N_E}{2\pi\Delta}$ |
|---|---|---|---|---|
| $E_{20}$ | 170.09 | 2.0 | 21.70 | 13.54 |
| $E_{21}$ | 196.68 | 2.5 | 22.68 | 12.52 |
| $E_{22}$ | 182.72 | 2.0 | 23.71 | 14.54 |
| $E_{23}$ | 205.06 | 2.5 | 24.49 | 13.05 |
| $E_{24}$ | 219.93 | 2.5 | 25.57 | 14.00 |
| $E_{28}$ | 325.90 | 3.2 | 31.30 | 16.21 |

**Table 1.** Computed upper bounds for the ranks of some curves, along with a heuristic guess of what these bounds should for a typical elliptic curve. The sum over the zeros here is rounded up; other numbers are rounded to nearest.

the methods described above, we compute rank bounds for each of these curves. These are listed in Table 1. The global root number can be computed for each curve. (In Sage, `E.root_number()`, which uses PARI [18], will finish quickly for $E_{20}$, $E_{21}$, and $E_{22}$ and within a few hours for $E_{23}$ and $E_{24}$. For $E_{28}$ it is best to see the mailing list discussion which gives the factorization of the discriminant [7].) In each case the root number agrees with the parity of the known number of independent points, so to get a tight upper bound for the rank we only need to get within 2 of the number of known independent points, and so the computation in Table 1 gives the proof of Theorem 1.1.

**2C.** ***Curves of small conductor.*** For further testing, this method was also run on all elliptic curves up with conductor below 180000 (from Cremona's tables [4]) using $\Delta = 2.0$, a computation which ran in under a day on a fast 8 core computer. In this range there are 790677 isogeny classes of elliptic curves, and for all but 9882 isogeny classes it turns out that

$$\left\lfloor \sum_\gamma f(\gamma; 2.0) \right\rfloor = \operatorname{rank}(E);$$

in the remaining cases,

$$\left\lfloor \sum_\gamma f(\gamma; 2.0) \right\rfloor = \operatorname{rank}(E) + 1,$$

so consideration of the root number of the curve gives the exact rank.

## 3. Further comments

**3A.** ***Some evidence towards BSD.*** There is a way in which these computations can be seen as giving mild evidence in support of the Birch and Swinnerton-Dyer conjecture. The upper bound computed for a curve $E$ is the value of the sum

$\sum_\gamma f(\gamma;\Delta)$, and as $f(\gamma;\Delta)$ decays fairly rapidly as $\gamma$ grows, one does not expect this sum to be very large for a typical elliptic curve.

To obtain a crude approximation to what we might expect the value of this sum to be, consider that the local zero density of a typical $L(s, E)$ near the central point is approximately $2\pi/\log N_E$. Then, if the zeros are spaced uniformly at random (an assumption that is not really correct, but is close enough to true for our crude purposes), we might expect that

$$\sum_\gamma f(\gamma,\Delta) \approx \frac{\log N_E}{2\pi}\int_{-\infty}^{\infty} f(t;\Delta)\mathrm{d}t = \frac{\log N_E}{2\pi\Delta},$$

possibly with a small adjustment to take into account the parity of the rank. (More precisely, we might expect that if we average this sum over all elliptic curves of conductor close to $N_E$, the answer will not be too far from this integral.) Thus, when this sum is significantly larger than this estimate, it indicates an extreme concentration of zeros near the central point. (It is also possible to arrive at more refined version of this heuristic by considering the explicit formula. In such a case, it is necessary to assume that the family of elliptic curves considered is large enough that $a_p(E)$ averages to zero for each $p$, and we notice that the integral of the $\Gamma$-factor plays a small role as well.)

As some further small evidence for this heuristic, we note that the average of

$$\frac{4\pi}{\log N}\sum_\gamma f(\gamma;2.0)$$

over all isogeny classes up to 180000 is approximately .9638. The small difference from 1 should be accounted for by the $\Gamma$-factor, which tends to push zeros away from the central point.

It should also be possible to refine this heuristic somewhat to make a guess as to what the sum should be for a high rank curve by making the assumption that a zero of high order at the central point will push other zeros away.

**3B.** ***Correctness tests.*** The method described here is simple enough that it is easy to implement, which reduces the likeliness of bugs. It is still important to test it where possible, however, in order to have more confidence in its correctness.

As described in Section 2C, this code was run on every isogeny class up to conductor 180000, and the fact that the computed upper bound for the rank was never too small gives some confidence that the computation was done correctly. As a further test, one can also compute many zeros for the $L$-function of an elliptic curve of small conductor, compute the sum over zeros directly, and verify that it agrees with our explicit formula implementation. Table 2 lists some example curves with small conductor for which this was done. The agreement there is

| $\Delta$ | $E$ | # zeros | Direct | Equation (2) | Difference |
|---|---|---|---|---|---|
| 2.0 | 11a | 200000 | 0.00270875 | 0.00269961 | $9.17 \times 10^{-6}$ |
| | 15a | 200000 | 0.00483749 | 0.00482836 | $9.13 \times 10^{-6}$ |
| | 17a | 200000 | 0.00559516 | 0.00558605 | $9.11 \times 10^{-6}$ |
| | 37a | 200000 | 1.00369174 | 1.00368272 | $9.01 \times 10^{-6}$ |
| | 118a | 200000 | 1.00636141 | 1.00635255 | $8.86 \times 10^{-6}$ |
| | 389a | 159650 | 2.00947449 | 2.00946618 | $8.30 \times 10^{-6}$ |
| | 5077a | 85520 | 3.01508240 | 3.01507647 | $5.92 \times 10^{-6}$ |
| | 11197a | 70950 | 3.02102728 | 3.02102250 | $4.77 \times 10^{-6}$ |
| 2.5 | 11a | 200000 | 0.00172459 | 0.00172653 | $1.94 \times 10^{-6}$ |
| | 15a | 200000 | 0.00170962 | 0.00171159 | $1.96 \times 10^{-6}$ |
| | 17a | 200000 | 0.00250017 | 0.00250215 | $1.97 \times 10^{-6}$ |
| | 37a | 200000 | 1.00335149 | 1.00335352 | $2.03 \times 10^{-6}$ |
| | 118a | 200000 | 2.00585774 | 2.00586023 | $2.49 \times 10^{-6}$ |
| | 389a | 159650 | 3.00797500 | 3.00797902 | $4.02 \times 10^{-6}$ |
| | 5077a | 85520 | 1.00543612 | 1.00543825 | $2.14 \times 10^{-6}$ |
| | 11197a | 70950 | 3.01798029 | 3.01798504 | $4.75 \times 10^{-6}$ |

**Table 2.** Sum of $f(\gamma; 2.0)$ and $f(\gamma; 2.5)$ computed directly with many zeros and using our implementation of (2). The curve labels correspond to isogeny classes in Cremona's tables [4] and the zeros were computed using Rubinstein's `lcalc` [20].

between $10^{-5}$ and $10^{-6}$, which is roughly the precision to which the integral in the explicit formula was calculated, and is in line with what should be expected using what is a fairly small number of zeros.

## Acknowledgments

Most of the computations in this paper run in a short amount of time, and were done on the author's personal computer. Some longer computations were run on the sage cluster at the University of Washington, supported by NSF grant DMS-0821725, and the riemann cluster at the University of Waterloo, funded by the Canada Foundation for Innovation, the Ontario Innovation Trust, and SGI.

The source code for our implementation is available as part of PSAGE [21]. It uses Sage [22], and hence PARI [18], to compute $a_p$ for bad primes, and uses Andrew Sutherland's `smalljac` [23] to compute all other values of $a_p$.

Parts of this work began while the author was in residence at the Mathematical Sciences Research Institute during the Arithmetic Statistics program, Spring 2011, during which time the author was partially supported by NSF grant DMS-0441170,

administered by MSRI. Discussions during the informal "explicit formula seminar," especially with David Farmer and Michael Rubinstein, were influential in encouraging this work.

Currently the author is supported by NSF grant DMS-0757627, administered by the American Institute of Mathematics.

The author would also like to thank Allan MacLeod for pointing out a small but important typo in an earlier version of this paper.

## References

[1] Andrew R. Booker, *Artin's conjecture, Turing's method, and the Riemann hypothesis*, Experiment. Math. **15** (2006), no. 4, 385–407. MR 2007k:11084

[2] Christophe Breuil, Brian Conrad, Fred Diamond, and Richard Taylor, *On the modularity of elliptic curves over* $\mathbb{Q}$*: Wild* 3*-adic exercises*, J. Amer. Math. Soc. **14** (2001), no. 4, 843–939. MR 2002d:11058

[3] Joe P. Buhler, Benedict H. Gross, and Don B. Zagier, *On the conjecture of Birch and Swinnerton-Dyer for an elliptic curve of rank* 3, Math. Comp. **44** (1985), no. 170, 473–481. MR 86g:11037

[4] John Cremona, *Elliptic curve data*, 2012. http://homepages.warwick.ac.uk/staff/J.E.Cremona/ftp/data/INDEX.html

[5] ———, `mwrank`, 2012. http://homepages.warwick.ac.uk/∼masgaj/mwrank/

[6] Andrej Dujella, *History of elliptic curve rank records*, 2012. http://web.math.hr/∼duje/tors/rankhist.html

[7] Noam Elkies, John Cremona, Bruce Dodson, Koh-ichi Nagao, and Bjorn Poonen, *Z^28 in E(Q), etc.*, NMBRTHRY listserv, 2006. http://tinyurl.com/ElkiesEtAlZ28

[8] Noam D. Elkies, *Elliptic curves and surfaces of high rank*, *I*, *II*, *III*, Tech. Report 34/2007, Mathematisches Forschungsinstitut Oberwolfach, 2007, expanded version at arXiv:0709.2908 [math.NT]. http://www.mfo.de/document/0729/OWR_2007_34.pdf

[9] Stéfane Fermigier, *Étude expérimentale du rang de familles de courbes elliptiques sur* $\mathbb{Q}$, Experiment. Math. **5** (1996), no. 2, 119–130. MR 98g:11061

[10] ———, *Une courbe elliptique définie sur* $\mathbb{Q}$ *de rang* $\geq 22$, Acta Arith. **82** (1997), no. 4, 359–363. MR 98j:11041

[11] Henryk Iwaniec and Emmanuel Kowalski, *Analytic number theory*, American Mathematical Society Colloquium Publications, no. 53, American Mathematical Society, Providence, RI, 2004. MR 2005h:11005

[12] Roland Martin and William McMillen, *An Elliptic Curve/Q of rank* 23, NMBRTHRY listserv, 16 March 1998. http://tinyurl.com/MartinMcMillen1

[13] ———, *An Elliptic Curve over Q with Rank at least* 24, NMBRTHRY listserv, 2 May 2000. http://tinyurl.com/MartinMcMillen2

[14] Jean-François Mestre, *Formules explicites et minorations de conducteurs de variétés algébriques*, Compositio Math. **58** (1986), no. 2, 209–232. MR 87j:11059

[15] F. Mezzadri and N. C. Snaith (eds.), *Recent perspectives in random matrix theory and number theory*, London Mathematical Society Lecture Note Series, vol. 322, Cambridge University Press, Cambridge, 2005. MR 2006c:11002

[16] Koh-ichi Nagao, *An example of elliptic curve over* $\mathbb{Q}$ *with rank* $\geq 20$, Proc. Japan Acad. Ser. A Math. Sci. **69** (1993), no. 8, 291–293. MR 95a:11052

[17] Koh-ichi Nagao and Tomonori Kouya, *An example of elliptic curve over $\mathbb{Q}$ with rank $\geq 21$*, Proc. Japan Acad. Ser. A Math. Sci. **70** (1994), no. 4, 104–105. MR 95e:11063

[18] The PARI Group, *PARI/GP* (*version* 2.4.3), 2011. http://pari.math.u-bordeaux.fr/

[19] Michael Rubinstein, *Computational methods and experiments in analytic number theory*, in Mezzadri and Snaith [15], 2005, pp. 425–506. MR 2006d:11153

[20] Michael O. Rubinstein, `lcalc`, 2012. http://code.google.com/p/l-calc/

[21] W. A. Stein et al., *Purple SAGE*, 2011. http://purple.sagemath.org

[22] ———, *Sage Mathematics Software* (*version* 4.7.2), 2011. http://www.sagemath.org

[23] Andrew Sutherland, `smalljac`, 2012. http://www-math.mit.edu/∼drew/

[24] Richard Taylor and Andrew Wiles, *Ring-theoretic properties of certain Hecke algebras*, Ann. of Math. (2) **141** (1995), no. 3, 553–572. MR 96d:11072

[25] Andrew Wiles, *Modular elliptic curves and Fermat's last theorem*, Ann. of Math. (2) **141** (1995), no. 3, 443–551. MR 96d:11071

JONATHAN W. BOBER: `jwbober@gmail.com`
*Department of Mathematics, University of Washington, Seattle, WA 98195-4350, United States*
*Current address*: *Howard House, University of Bristol, Queens Avenue, Bristol BS8 1SN United Kingdom*

VOLUME EDITORS

Everett W. Howe
Center for Communications Research
4320 Westerra Court
San Diego, CA 92121-1969
United States

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

---



ISSN: 2329-9061 (print), 2329-907X (electronic)

ISBN: 978-1-935107-00-2 (print), 978-1-935107-01-9 (electronic)

First published 2013.

---

**MATHEMATICAL SCIENCES PUBLISHERS**
798 Evans Hall #3840, c/o University of California, Berkeley CA 94720-3840
contact@msp.org **http://msp.org**

# THE OPEN BOOK SERIES 1

# Tenth Algorithmic Number Theory Symposium

The Algorithmic Number Theory Symposium (ANTS), held biennially since 1994, is the premier international forum for research in computational number theory. ANTS is devoted to algorithmic aspects of number theory, including elementary, algebraic, and analytic number theory, the geometry of numbers, arithmetic algebraic geometry, the theory of finite fields, and cryptography.

This volume is the proceedings of the tenth ANTS meeting, held July 9–13, 2012, at the University of California, San Diego. It includes revised and edited versions of the 25 refereed papers presented at the conference, together with extended abstracts of two of the five invited talks.

## TABLE OF CONTENTS