A Database of Elliptic Curves – First Report

William A. Stein[1] and Mark Watkins[2]

[1] Harvard University
was@math.harvard.edu
http://modular.fas.harvard.edu
[2] The Pennsylvania State Univerisity
watkins@math.psu.edu
http://www.math.psu.edu/watkins

1 Introduction

In the late 1980s, Brumer and McGuinness [2] undertook the construction of a database of elliptic curves whose absolute discriminant $|\Delta|$ was both prime and satisfied $|\Delta| \leq 10^8$. While the restriction to primality was nice for many reasons, there are still many curves of interest lacking this property. As ten years have passed since the original experiment, we decided to undertake an extension of it, simultaneously extending the range for the type of curves they considered, and also including curves with composite discriminant. Our database can be crudely described as being the curves with $|\Delta| \leq 10^{12}$ which either have conductor smaller than 10^8 or have prime conductor less than 10^{10}—but there are a few caveats concerning issues like quadratic twists and isogenous curves. For each curve in our database, we have undertaken to compute various invariants (as did Brumer and McGuinness), such as the Birch–Swinnerton-Dyer L-ratio, generators, and the modular degree. We did not compute the latter two of these for every curve. The database currently contains about 44 million curves; the end goal is find as many curves with conductor less than 10^8 as possible, and we comment below on this direction of growth of the database. Of these 44 million curves, we have started a first stage of processing (computation of analytic rank data), with point searching to be carried out in a later second stage of computation.

Our general frame of mind is that computation of many of the invariants is rather trivial, for instance, the discriminant, conductor, and even the isogeny structure. We do not even save these data, expecting them to be recomputable quite easily in real time. For instance, for each isogeny class, we store only one representative (the one of minimal Faltings height), as we view the construction of isogenous curves as a "fast" process. It is only information like analytic ranks, modular degrees (both of which use computation of the Frobenius traces l_p), and coordinates of generators that we save; saving the l_p themselves would take too much storage space. It might be seen that our database could be used a "seed" for other more specialised databases, as we can quickly calculate the less time-consuming information and append it to the saved data.

C. Fieker and D.R. Kohel (Eds.): ANTS 2002, LNCS 2369, pp. 267–275, 2002.

2 Generating the Curves

While Brumer and McGuinness fixed the a_1, a_2, a_3 invariants of the elliptic curve (12 total possibilities) and then searched for a_4 and a_6 which made $|\Delta|$ small, we instead decided to break the c_4 and c_6 invariants into congruence classes, and then find small solutions to $c_4^3 - c_6^2 = 1728\Delta$. We write $c_4^\star$ for the least nonnegative residue of c_4 modulo 576, and $c_6^\star$ for the least nonnegative residue of c_6 modulo 1728. The work of Connell [3] gives necessary and sufficient conditions on c_4 and c_6 for an elliptic curve with such invariants to exist. We first need that $c_6 \equiv 3 \pmod 4$ (when it follows that c_4 is odd) or $2^4 \mid c_4$ and $c_6 \equiv 0, 8 \pmod{32}$, and secondly we require a local condition at the prime 3, namely that $c_6 \not\equiv \pm 9 \pmod{27}$. Using this information and the fact that $1728 \mid \left(c_4^3 - c_6^2\right)$, this leads to 288 possible $(c_4^\star, c_6^\star)$ pairs.

For each fixed such $(c_4^\star, c_6^\star)$ pair, we can simply loop over c_4 and c_6, finding the curves with $|\Delta| \le 10^{12}$. Of course, it is only under the ABC-conjecture that we would have an upper bound on c_4 to ensure that we would have found all such curves, and even then the bound would be too large. Our method was to take $c_4 \le 1.44 \cdot 10^{12}$ in this first step; in any case, curves with larger c_4 are most likely found more easily using the method of Elkies [5].

2.1 Minimal Twists

In the sequel, we shall write E_d for the quadratic twist of E by d. For each (c_4, c_6) pair (again with $c_4 \le 1.44 \cdot 10^{12}$) which satisfies the $|\Delta| \le 10^{12}$ condition, we then determine whether this curve is minimal—not only in the traditional sense for its minimal discriminant, but also whether it is has the minimal discriminant in its family of quadratic twists. For $p \ge 5$, this is rather easy to determine; unless $p^6 \mid \Delta$ and $p \mid c_4$, the curve is minimal for quadratic twists (the only difference between this and the standard notion of minimality is that the exponent here is 6 instead of 12). If both the above conditions hold, then we throw the curve out, as $E_{\tilde{p}}$, where $\tilde{p} = \left(\frac{-1}{p}\right) p$, is a curve with lesser discriminant (which will be found by our search procedure). Given that the curve is minimal at a prime divisor $p \ge 5$ of Δ, the local conductor at p is p^2 if $p \mid c_4$ and p^1 otherwise.

The case with $p = 3$ is a bit harder. By Connell's conditions, we see that if $3 \mid c_6$ and $3^9 \mid \left(c_4^3 - c_6^2\right)$ but 3^5 does not exactly divide c_6, then E_{-3} is a curve with invariants $(c_4/9, -c_6/27)$ which has the discriminant reduced by 3^6. This is the only prohibition against the curve being the minimal twist at 3. If $3 \,||\, c_4$, the curve has good reduction (at 3), while if c_4 is not divisible by 3, the curve has either good or multiplicative reduction. In both cases, the local conductor can be computed readily, it being 3^0 for good reduction and 3^1 for multiplicative. To compute the conductor in the remaining cases of additive reduction (where we know that $3^2 \mid c_4$ and $3^3 \mid c_6$), let $\tilde{c}_4$ be the the least nonnegative residue of $(c_4/9)$ modulo 3, and $\tilde{c}_6$ be the the least nonnegative residue of $(c_6/27)$ modulo 9. Table 1 then gives us the exponent of the local conductor. Here $e = 5$ if $3^4 \mid c_4$ and $e = 4$ if $3^3 \,||\, c_4$ (note that we must have $3^5 \,||\, c_6$ in this case for the curve to be twist-minimal, and that the table assumes that the curve is twist-minimal).