How many elliptic curves can have the same prime conductor?

Alberta Number Theory Days, BIRS, 11 May 2013

Noam D. Elkies, Harvard University

Review: Discriminant and conductor of an elliptic curve

Finiteness proofs: Hall/ABC (conjecturally!), modularity, Siegel, Thue(-Siegel-Roth)

Uniformity questions

Computations and new examples

Recall: elliptic curve = genus-1 curve with distinguished rational point O. Weierstrass form with O at infinity:

$$E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$

(away from characteristic 2 and 3 we may assume "narrow Weierstrass form" $y^2 = x^3 + a_4x + a_6$ with $a_1 = a_2 = a_3 = 0$). The subscripts are weights: scaling (x, y) to $(\lambda^2 x, \lambda^3 y)$ multiplies each a_i by λ^i.

The discriminant is a polynomial $\Delta = \Delta(E) = 12^{-3}(c_4^3 - c_6^2)$ of weight 12 in the a_i; here c_4, c_6 are polynomials of weights 4 and 6, and for $y^2 = x^3 + a_4x + a_6$ simply $c_4 = -48a_4$ and $c_6 = -864a_6$, so $\Delta = 16\,\mathrm{disc}_x(x^3 + a_4x + a_6)$. A (smooth) elliptic curve has $\Delta \neq 0$.

NB outside characteristic 2 or 3, two elliptic curves E, E' are isomorphic iff there exists rational λ such that $c_4(E') = \lambda^4 c_4(E)$ and $c_6(E') = \lambda^6 c_6(E)$.

Now suppose $a_i \in \mathbf{Q}$. Scaling (x, y) to $(\lambda^2 x, \lambda^3 y)$ yields an isomorphic elliptic curve with each a_i multiplied by λ^i. We may choose λ so that each $a_i \in \mathbf{Z}$. Then also $\Delta \in \mathbf{Z}$. The minimal Δ (over isomorphic curves with integral a_i) is the discriminant of E; it can be computed using Tate's algorithm. The prime factors p of Δ are those such for which E becomes singular (has "bad reduction") mod p, and the valuation $v_p(\Delta)$ is a measure of the complexity of this singularity. These p include all factors of the denominator of the j-invariant of E.

The conductor $N = N(E)$ is a subtler invariant. It has the same prime factors as Δ, but with $v_p(N) \leq v_p(\Delta)$ for all p; indeed each $v_p(N)$ is bounded: $v_2 \leq 8$, $v_3 \leq 5$, and $v_p \leq 2$ for all $p > 3$. The conductor distinguishes multiplicative from additive reduction: if E has multiplicative reduction mod p then $v_p(N) = 1$ ("$p \,\|N$"); if additive, $v_p(N) \geq 2$ (and $p^2 \,\|N$ if $p > 3$.) If $p > 3$ then E has additive reduction mod p iff c_4 and c_6 are both 0 mod p. The conductor is defined to be always positive (more canonically, it's the norm of a "conductor ideal"), unlike Δ which may have either sign.

Unlike Δ, the conductor N is invariant under isogeny: two elliptic curves related by an isogeny over $\mathbf{Q}$ have the same N. It is N, not Δ, that enters the functional equation for $L(E, s)$ and gives the level of the modular form associated to E and its modular parametrization by $X_0(N)$.

As with number fields, the sizes of Δ and N also measure in different ways the complexity of E. We would hope, then, that any upper bound on $|\Delta|$ or N restricts E to a finite list. This is true but not easy.

The easy finiteness result is on curves with bounded *height*, which we may define by

$$H(E) = \max(|c_4(E)|^3, |c_6(E)|^2)$$

so for large M there are about $CM^{5/6}$ curves of height at most M. Since $12^3\Delta = c_4^3 - c_6^2$, certainly $|\Delta(E)| \leq 12^{-3}H(E)$, but Δ could be considerably smaller; a famous example of such cancellation is the curve with

$$(a_1, a_2, a_3, a_4, a_6) = (0, -1, 1, -7820, -263580),$$

which has $c_4 = 375376$, $c_6 = 229985128$, and $\Delta = -11$. (Such curves are nearly singular at the Archimedean prime, which is not detected by Δ or N.)

For N, the question is even harder, because one could imagine a sequence of curves with constant N but ever-larger Δ.

So why might we believe that each Δ, and even each N, occurs for only finitely many E?

Hall's conjecture bounds the cancellation in $12^3\Delta = c_4^3 - c_6^2$, asserting that for all $\theta < 1/2$ the inequality $|a^3 - b^2| > a^\theta$ holds for all but finitely many integers $a, b > 0$ for which $a^3 \neq b^2$. This would make $\Delta > H^{\theta/3}$ with finitely many exceptions, thus bounding c_4 and c_6 and proving what we want.

The **ABC conjecture** generalizes Hall, and implies $N > H^{\theta/3}$ with finitely many exceptions for each $\theta < 1/2$, which would prove that N is the conductor of finitely many elliptic curves as desired.

Recall that the ABC conjecture asserts that for each $\epsilon > 0$ there are only finitely many coprime triples (A, B, C) of integers such that $A+B+C = 0$ and $\mathcal{N}(A, B, C) < \mathcal{H}(A, B, C)^{1-\epsilon}$, where $\mathcal{H}$ is the height

$$\mathcal{H}(A, B, C) := \max(|A|, |B|, |C|)$$

and $\mathcal{N}$ is the conductor

$$\mathcal{N}(A, B, C) := \prod_{p|ABC} p$$

without multiplicity [so called because, up to a bounded power-of-2 factor, this is the conductor of the associated Frey curve $Y^2 = X(X - A)(X + B)$ of discriminant $16(ABC)^2$].

The idea is that if $a^3 - b^2 = D$ then we take $(A, B, C) = (-a^3, b^2, D)$. If a, b are coprime (or at least have bounded gcd) then $\mathcal{H} \sim H$ and $\mathcal{N} \lesssim H^{5/6}N$, so ABC gives $N \gg H^{\frac{1}{6}-\epsilon}$.

Dropping the assumption that a, b are coprime, we still start from $(-a^3, b^2, D)$ but then divide by $d := \gcd(a^3, b^2)$ and apply the ABC conjecture to $(A, B, C) = (-a^3/d, b^2/d, D/d)$. Then $\mathcal{N}(D/d)$ is not quite N, because (for $p > 3$) if $p|d$ then E has additive reduction at p so $v_p(N) = 2$, whereas $\mathcal{N}(D/d)$ has p-valuation 1, or even 0 if $v_p(a) = 2$ and $v_p(b) = 3$. We also need to use $v_p(d) < 12$ (else $p^4|a$ and $p^6|b$ and our model $y^2 = x^3 + ax + b$ for E is not minimal at p). After some bookkeeping we find that $N \gg H^{\frac{1}{6}-\epsilon}$ still holds in this generality as well.

[This is one direction of the equivalence between ABC and the "modified Szpiro conjecture"; the other direction uses the Frey curve $Y^2 = X(X - A)(X + B)$.]

But ABC and even Hall are still only conjectures. . .

Modularity, on the other hand, is a theorem: up to isogeny, curves of conductor $N \longleftrightarrow$ 1-dim. factors of the Jacobian of $X_0(N)$. So the genus of $X_0(N)$ is an upper bound on the number of isogeny classes. Moreover it's known that any isogeny class of elliptic curves is finite. This proves finiteness of the set of elliptic curves of given N (and thus also of given Δ), and even gives an upper bound on its size, namely 8 times the genus of $X_0(N)$ (which is $N^{1+o(1)}$, and usually $O(N)$ — though the uniform upper bound on the size of an isogeny class is a hard theorem of Mazur).

But the modularity of every elliptic curve over $\mathbf{Q}$ is a rather recent and *really*$^{\otimes 2}$ hard theorem. . .

Fortunately much older (though still nontrivial) theorems are all that we need.

Given Δ, the equation $c_4^3 - c_6^2 = 12^3\Delta$ itself gives an elliptic curve, call it $\mathcal{E}_\Delta$. Thus curves with discriminant Δ correspond to integral points on $\mathcal{E}_\Delta$. (That's an injection but not a bijection, because c_4, c_6 must satisfy some congruence criteria to come from an elliptic curve; we shall return to this.) But by a theorem of Siegel *any* elliptic curve has only finitely many integral points.

Given N, there are finitely many possibilities for Δ mod $(\mathbf{Q}^*)^6$. The resulting points on each $\mathcal{E}_\Delta$ need not be integral, but they're S-*integral* for $S = \{p \text{ prime}: p|N\}$. Hence they too are finite in number.

Alternatively we can reduce the problem to a Thue equation. (Such a reduction is available for any elliptic curve, but it's particularly simple for $\mathcal{E}_\Delta$.) Write the equation as

$$c_4^3 = c_6^2 + 12^3\Delta = (c_6 + u)(c_6 - u)$$

where $u = \sqrt{-12^3\Delta}$. Let K be the (usually quadratic) number field $\mathbf{Q}(u)$, and O_K its ring of integers, which contains $c_6 \pm u$. Any common factor of $c_6 + u$ and $c_6 - u$ must divide their difference $2u$ (that is, any ideal of O_K that contains both $c_6 \pm u$ must contain $2u$). This restricts $c_6 \pm u$ to a finite set modulo $(K^*)^3$, each of which yields a cubic Thue equation (that is, a Diophantine equation $P(m,n) = d$ where d is fixed and P is a homogeneous cubic without repeated roots). We then reach our goal using Thue's theorem that such an equation of any degree > 2 has finitely many integral solutions. Likewise for elliptic curves of conductor N, via finiteness of S-integral solutions of a cubic Thue equation.

For example, for $\Delta = -11$ we have $u = 24\sqrt{33}$, so

$$K = \mathbf{Q}(\sqrt{33}), \qquad O_K = \mathbf{Z}[\frac{1}{2}(1+\sqrt{33})],$$

and $c_6 \pm u$ must be cubes up to factors of $2u$. One of the possible $c_6 + u$ mod cubes is $\alpha := 17 - 3\sqrt{33}$ (with norm -8). Taking $z = m + n\sqrt{33}$ in $c_6 + u = \alpha z^3$ and expanding yields

$$-3m^3 + 51m^2n - 297mn^2 + 561n^3 = 24,$$

to be solved in $m, n \in \mathbf{Z}$ or $m, n \in \mathbf{Z} + \frac{1}{2}$. The solution $(c_4, c_6) = (375376, 229985128)$ comes from $(m, n) = (403, 103)$. There are three smaller solutions $(m, n) = (-2, 0)$, $(-5, -1)$, and $(-8, -2)$, corresponding to $(c_4, c_6) = (-8, \pm 136)$, $(16, \pm 152)$, and $(136, \pm 1592)$; of these $(16, -152)$ comes from the elliptic curve $X_1(11) : y^2 + y = x^3 - x^2$ of discriminant -11, and the others fail a congruence condition (e.g. $c_4 = -8$ or $c_4 = 136$ are even but not 0 mod 16).

Note on effectivity: The original proofs of Siegel's and Thue's theorems gave effective bound on the *number* of integral points, but not on their size, nor algorithms for provably generating all of them. This is because in each case it takes at least two very large solutions to get a contradiction, but we don't expect to see even one.

By now, though, effective and computationally efficient proofs are available for both Siegel and Thue. However, for Siegel one must first compute the group of rational points on $\mathcal{E}_\Delta$, and it's not yet known that that can always be done (though in practice we can usually do it if Δ is not too large). For Thue the algorithm is unconditional, as is the reduction via class groups and S-units of K; indeed such a computation is also the first step of a "descent" to find $\mathcal{E}_\Delta(\mathbf{Q})$.

So, for each Δ or N there are finitely many curves of discriminant Δ or conductor N. But is this finite number uniformly bounded as we vary Δ or N?

Naïve probabilistic guess: yes, because for large M the number of curves of conductor or discriminant up to M should be $M^{(5/6)+o(1)}$, i.e. a random integer H is a discriminant or conductor with probability $|H|^{o(1)-(1/6)}$. If these are uncorrelated then 6-fold coincidences should be rare, and multiplicity 7 or more should be seen only finitely many times.

But the reality is more complicated . . .

Numerical evidence: all modular elliptic curves of conductor $N \leq H$ have been computed for $H = 200$ (Tingley: the "Antwerp Tables" at the back of LNM 476), then $H = 1000$ (Cremona), and by now Cremona has reached far enough to verify that rank 4 first occurs for $N = 234446$. So what do the multiplicities look like?

$N \leq 10$: none.
$N = 11$: three curves, all isogenous:
$\mathsf{X}_1(11)$, $\mathsf{X}_0(11)$, and $(0, -1, 1, -7820, -263580)$.
$N = 15$: eight curves, all isogenous to $\mathsf{X}_0(15)$.
$N = 66$: 12 curves 66A–66L, 3 isogeny classes
$N = 198$: 20 curves 198A–198T, 5 isogeny classes
Cremona 1000: run out of letters, so new labeling scheme,
e.g. 198A1–A4, . . . , 198E1–E4.
Cremona 10^4: run out again, so Y, Z, AA, BB, CC, . . .
Cremona 10^5: 274 isogeny classes for $N = 66150 = 2 \cdot 3^3 5^2 7^2$
66150NNNNNNNNNNN1 with 11 N's is "getting out of hand", change to 66150jn1

So, could it be that the count is unbounded, or is this yet another example where we expect small-N data to mislead? (For ranks we expect rank 0, 1, and 2+ to happen for 50%, 50%, and 0% of all curves, but tables seem to show the average rank climbing slowly towards 1.)

In fact it's not hard to prove that there are arbitrarily large sets of elliptic curves with the same N. This is true even for the curves $\mathcal{E}_\Delta$. These always have conductor $2^b 3^c \prod_p p^2$ with p ranging over the primes $p > 3$ s.t. $v_p(\Delta) \not\equiv 0 \bmod 6$, so we can easily arrange for huge "coincidences".

Likewise for curves of the form $y^2 = x^3 + a_4 x$, or quadratic twists $\mu y^2 = x^3 + a_4 x + a_6$ for fixed a_4, a_6 such that the $\mu = 1$ curve has additive reduction at many primes.

But that's the only way we know to generate arbitrarily many curves with the same conductor. If we insist that the curves have distinct j-invariants then the uniformity question is open. That's in particular the case when N is squarefree (a.k.a. E is "semistable"), even though large packets of same-N curves have been observed even in this case when the number of prime factors is large.

(Heuristic explanations: more prime factors mean more choices for Δ, and also more Atkin-Lehner factors of $\mathrm{Jac}(X_0(N))$. But both effects should be negligible for really large N.)

For another reason, we expect arbitrarily large sets of elliptic curves with the same Δ. Choose Δ_0 such that $\mathcal{E}_{\Delta_0}$ has positive rank (again $\Delta = -11$ works, with rank 2). We may assume Δ_0 free of sixth powers. There are then infinitely many solutions of $c_4^3 - c_6^2 = 12^3\Delta_0$ in *rational* c_4, c_6, necessarily with denominators d^2, d^3 for some $d \in \mathbf{Z}$. Choose some that are squarefree and coprime to 6. (This should happen infinitely often for some Δ_0, including -11, though we cannot prove it). Let D be the least common multiple of these d, and $\Delta = D^6\Delta_0$, which is free of 12th powers. Then $\mathcal{E}_\Delta \cong \mathcal{E}_{\Delta_0}$, and the isomorphism takes each of our (c_4, c_6) to an integral solution of $c_4^3 - c_6^2 = \Delta$, and thus to an elliptic curve of discriminant Δ or $2^{12}\Delta$. So one of these should arise as many times as we like. (NB the conductor will in general still take many different values on these curves.)

We can now see why it restricting to prime N and $|\Delta|$ is not just numerology but a natural question: this avoids the tricks that we saw when there are repeated factors, and (for prime N) also avoids the issue of Atkin-Lehner signs that may obscure the large-N behavior.

Some further features:

1) Mestre-Oesterlé theorem: If N is prime then $|\Delta| = N$, except that Δ can be 11^5, 17^2 or 17^4, 19^3, 37^3, and p^2 for $p = n^2 + 64$; and the last of these happens only once for each such prime p (Setzer-Neumann curves). So the uniformity question is the same for prime $|\Delta|$ and prime N.

2) Computing all modular curves of conductor N is somewhat easier when N is prime ("méthode des graphes", etc.), and more extensive tables are available.

The prime case might also be particularly amenable to the techniques of Caporaso-Harris-Mazur and Abramovich, but so far it's not known that the number of integral solutions of $c_4^3 - c_6^2 = \pm 12^3 p$ is uniformly bounded as the prime p varies.

The congruence conditions on c_4 and c_6 are also quite simple in this prime case; for instance if $\Delta = \pm 1 \bmod 9$ then c_4 must be either odd or a multiple of 16, and then exactly one of $\pm c_6$ works.

So what do computations find?

The counts are still increasing, though much more slowly. There are seven curves of conductor 28279, and (at least) thirteen for 61263451 (A.Brumer, published in his paper with Silverman 1996).

Computing power is much greater since 1996, and some relevant software is much improved too, so it's worth looking again.

First idea: trawl through the $H^{5/6}$ pairs (c_4, c_6) with $c_4 \ll H^{1/2}$ and $c_6 \ll H^{1/3}$ that satisfy the appropriate congruence, and whenever $|\Delta|$ is prime dump it to a file. Then sort the file in time about $H^{5/6}$ and seek duplicates. For high multiplicities, search beyond $H^{1/3}$ to seek solutions with large cancellation in $c_4^3 - c_6^2 = 1728\Delta$.

This works for a while, but $H^{5/6}$ is a lot of space.

Better idea: most of that work and space is wasted on Δ that arise only once, so look for pairs, of which there should be only about $H^{2/3}$. That is, for each c_4, c_4' solve $c_4^3 - c_6^2 = {c_4'}^3 - {c_6'}^2$ by factoring $c_4^3 - {c_4'}^3$, and then dump the prime Δ's as before. This soon finds $\Delta = 14425386253757$ with at least 21 curves.

For the last search, I went up to 10^{15} but imposed congruence conditions $\Delta \equiv 1 \bmod 4$, $\Delta \equiv \pm 1 \bmod 9$ which were satisfied by practically all of the high-multiplicity Δ found previously. A week or so later, barely reached $\Delta = -998820191314747$ which occurs for at least 24 curves!

$$(a_1, a_2, a_3, a_4, a_6) = (1, -1, 0, 24955, 92748),$$
$$(0, 0, 1, 19930, -1067380),\ (1, -1, 0, 5299, 1511964),$$
$$(0, 0, 1, 4297, -1516684),\ (1, 0, 1, -5656, 1528869),$$
$$(0, 1, 1, -9673, 1560803),\ (0, 0, 1, -16475, 1724692),$$
$$(0, 1, 1, -20062, -1879756),\ (0, -1, 1, -36113, 3059917),$$
$$(0, 0, 1, -45554, -4039412),\ (0, 0, 1, -63590, 6356620),$$
$$(1, 1, 1, -69648, 7207292),\ (1, -1, 1, -103975, -12967734),$$
$$(0, -1, 1, -203192, -35219102), (0, -1, 1, -285863, 58943167),$$
$$(0, 1, 1, -295592, 61777014),\ (0, -1, 1, -350761, 80090069),$$
$$(0, 0, 1, -630914, -192893172),$$
$$(0, -1, 1, -8262736, 9144601514),$$
$$(0, 0, 1, -22950140, -42318096308),$$
$$(0, 0, 1, -34483919, -77942267852),$$
$$(1, 1, 1, -43977208, 112232514820),$$
$$(0, 0, 1, -106102229, 420663542788),$$
$$(0, -1, 1, -278805873, -179175434216 3).$$

But 24 and even 10^{15} are still far from ∞...

THANK YOU.