Elliptic curves over $\mathbb{Q}(\sqrt{5})$

with good reduction away from 2

R.G.E. Pinch

Cheltenham

28 April 2012

Outline

Elliptic curves over $\mathbb{Q}(\sqrt{5})$ with good reduction away from 2

Theorem. There are 49 values of the j-invariant and 416 isomorphism classes of elliptic curves over $F = \mathbb{Q}(\sqrt{5})$ with good reduction away from 2.

All such curves have integral j-invariant

There are no elliptic curves over F with everywhere good reduction.

Some finiteness theorems

- algebraic number fields with bounded degree and given set of ramified primes
- rank of the group of rational points on a given abelian variety over a number field
- abelian varieties over a number field of bounded dimension and given set of bad reduction
- points on a curve of genus ≥ 2 over a number field

Rational point of order 2

Let K be a field such that every quadratic extension of K ramified only over 2 has class number prime to 3. Then a cubic extension of K ramified only over 2 is tamely ramified.

There is no cubic extension of F ramified only at 2.
Proof. If not, the 2-division field L is a cubic extension of F ramified only at 2. The different of the extension of $L/\mathbb{Q}$ is computable, and ramification is tame. The absolute discriminant of L will then contravene the Hermite bound. □

Let E be an elliptic curve over F with good reduction away from 2. Then E has a point of order 2 defined over F.

Hautpmodul for order 2

The Hauptmodul τ for $X_0(2)$ parametrises elliptic curves with a subgroup of order 2.
We have

$$j = \frac{(\tau + 16)^3}{\tau}$$

$$j - 1728 = \frac{(\tau + 64)(\tau - 8)^2}{\tau}$$

with the isogenous curve corresponding to $\tau' = 4096/\tau$.

Hautpmodul for order 2

We have

$$\Delta = 2^{12} j^2 (j - 1728)^9 w^6$$

and since F has class number 1 there is a global minimal equation with Δ a power of 2 times a unit.

Good reduction away from 2 means that τ cannot be divisible by any prime other than (2). Further, in $\tau + 64$ the primes other than (2) occur to even powers.

Hautpmodul for order 2

Either τ or $\tau' = 4096/\tau$ satisfies one of the equations

$$t = 64u/v, \qquad u + v = 2x^2$$

or

$$t = 64v/2^a u, \qquad 2^a u + v = x^2$$

where u, v are units, $x \in F$ and $a \geq 0$.

Specific solutions

The equation

$$2x^2 = u + v, \qquad u, v \text{ units of } F,$$

has the solutions

a)	$x = 0$	$u = 1$	$v = -1$
b)	1	1	1
c)	1	ϵ^2	ϵ'
d)	3	ϵ^6	ϵ'^6

Specific solutions

The equations

$$x^2 = 2^a u + v, \qquad u, v \text{ units}, \quad a \geq 0,$$

have the solutions

e)	$a = 0$	$x = 0$	$u = 1$	$v = -1$
f)	0	1	ϵ	ϵ'
g)	0	1	ϵ^2	$-\epsilon$
h)	0	2	ϵ^3	ϵ'^3
i)	1	1	1	-1

Specific solutions

j)	1	1	$-\epsilon$	ϵ^3
k)	1	ϵ	1	$-\epsilon'$
l)	1	$\sqrt{5}$	ϵ^2	ϵ'^3
m)	1	$8+15\epsilon$	ϵ^{13}	ϵ'
n)	2	$\sqrt{5}$	1	1
o)	2	ϵ^3	ϵ^3	1
p)	3	3	1	1
q)	3	$5+2\sqrt{5}$	ϵ^5	1
r)	3	$3+2\sqrt{5}$	ϵ^4	1
s)	4	$17+8\sqrt{5}$	ϵ^9	1

An example equation

The simultaneous Diophantine equations

$$\begin{aligned} X^2 - 2Y^2 &= -1, \\ X^2 - 10Z^2 &= -9 \end{aligned}$$

have the solutions

$$(X, Y, Z) = (\pm 1, \pm 1, \pm 1) \text{ or } (\pm 41, \pm 29, \pm 13)$$

Another example

The simultaneous Diophantine equations

$$\begin{aligned}(X+2)^2 - 10Y^2 &= -1,\\ (X-2)^2 - 2Z^2 &= -1;\end{aligned}$$

have the solutions

$$(X, Y, Z) = (1, \pm 1, \pm 1) \text{ or } (-5, \pm 1, \pm 5);$$

Reminder on binary recurrence relations

A *binary recurrence relation*

$$X_{n+1} = aX_n + bX_{n-1}$$

(where we require $b = \pm 1$) has *auxiliary polynomial*

$$f(z) = z^2 - az - b$$

and general solution

$$X_n = c_1\alpha_1^n + c_2\alpha_2^n$$

where α_1, α_2 are the roots of f.

If f has repeated root α, then $X_n = (c_1 n + c_0)\alpha^n$.

Some more finiteness theorems

- approximations p/q to algebraic α with $\left|\alpha - \frac{p}{q}\right| < \frac{1}{q^{2+\epsilon}}$
- integer solutions to $f(x, y) = m$ where f of degree ≥ 3
- integer solutions to $F(x, y) = 0$ where F is of degree ≥ 3
- integral points on an elliptic curve over a number field

Linear forms in logarithms

Suppose $n \geq 2$ and that $\alpha_1, ..., \alpha_n$ are non-zero algebraic numbers of degree at most d, and height $H(\alpha_i)$ at most A, where $d \geq 4$, $A \geq 4$. Let $b_1, ..., b_n$ be rational integers. The linear form in logarithms

$$\Lambda = b_1 \log \alpha_1 + ... + b_n \log \alpha_n$$

Assuming that the form Λ is non-zero, we aim to bound Λ away from zero.
The current results are of the form

$$|\Lambda| > \exp(-C(\log A)^{\kappa} \log B)$$

where $\kappa = \kappa(n)$ and $C = C(n, d)$.

An inequality of Baker

Suppose $n \geq 2$ and that $\alpha_1, ..., \alpha_n$ are non-zero algebraic numbers of degree at most d, and height $H(\alpha_i)$ at most A, where $d \geq 4$, $A \geq 4$. If there are rational integers $b_1, ..., b_n$ such that

$$0 < b_1 \log \alpha_1 + ... + b_n \log \alpha_n < \exp(-\lambda B)$$

where $0 < \lambda \leq 1$ and $\max\{|b_1|, ..., |b_n|\} \leq B$, then

$$B < \left(4^{n^2} \log A \cdot \lambda^{-1}\right)^{(2n+1)^2}.$$

An inequality of Baker–Wüstholz

Let $\Lambda = b_1 \log \alpha_1 + ... + b_n \log \alpha_n$. We have

$$\log |\Lambda| > -(16nd)^{2(n+2)} (\log A)^n \log B$$

If there are rational integers $b_1, ..., b_n$ such that

$$0 < b_1 \log \alpha_1 + ... + b_n \log \alpha_n < \exp(-\lambda B)$$

where $0 < \lambda \leq 1$ and $\max\{|b_1|, ..., |b_n|\} \leq B$, then, if $B > 364800$, we have

$$B < \left((16nd)^{2(n+2)} (\log A)^n \lambda^{-1} \right)^{1.25}.$$

Verification

We consider the question of verifying that a list of solutions to a Diophantine equation is *complete*.
This might arise after a naive search for (small) solutions, or as a result of some other systematic search.

Verifying solutions

Suppose that X_m and Y_n are binary recurrent and we wish to prove that $(m, n) = (0, 0)$ is the only solution to $X_m = Y_n + g$. From Baker's method, we obtain a bound B such that any solution must satisfy $|m|, |n| < B$. We can deduce that $m = n = 0$ is the only solution if we can find integer moduli M, N, with $M, N > B$, such that $X_n = Y_m + g$ implies $M|m, N|n$. We need to find a set of primes p with associated exponents e such that implies $p^e|m$, and a similar set for n. To obtain M we perform step P for a suitable set of primes p.

Step P

Input. Moduli M, N for which $M|m$, $N|n$; prime p.
Output. Moduli M, Np, or M, N for which $M|m$, $N|n$.
Procedure. Suppose that p^{e-1} already divides N. Form a set S of possible values for m mod p^e: initially S will consist of the p multiples of p^{e-1}. Form a set Q of primes q such that the sequence (X_n) mod q has a cycle length exactly divisible by p^e. Perform Step Q for each q in Q until S is reduced to the single element 0, in which case return moduli Mp, N, or else fail, in which case return M,N.

Step Q

Input. Prime q such that (X_n) mod q has cycle length exactly divisible by p^e; set S of values modp^e such that n mod p^e is in S.
Output. Modified set $S' \subset S$ such that n mod p^e is in S'.
Procedure. Let the cycle lengths of $(X), (Y)$ mod q be ℓ_X, ℓ_Y respectively, and let $h_X = \mathrm{hcf}\{N, \ell_X\}$, $h_Y = \mathrm{hcf}\{M, \ell_Y\}$. Let V be the set of values $Y_m + g$ mod q for m between 1 and ℓ_Y with m divisible by h_Y. Let S' initially be the set $\{0\}$. For n from 1 to ℓ_X with n divisible by h_X and n mod p^e in S, add n mod p^e to S' if X_n mod q is in V. Return S'.

Algorithm A

Input. Two unital recurrent sequences (X_n), (Y_m), an integer g such that $X_0 = Y_0 + g$.
Output. Integers M, N such that $X_n = Y_m + g$ implies M divides m, N divides n.
Procedure. Take a list L of primes to use as candidates for the modulus q of step Q and compute the cycle lengths ℓ_X , ℓ_Y of X, Y modulo (q) for every prime in L. Take a list H of primes to use as the possible factors p of M and N. Set M and N initally to 1. Repeat steps R and R' until no more primes can be added to M and N. Output M, N.
R) For each prime p in H, and for each power e of p, perform step P for p^e using the primes of L to form the set Q, taking the next prime from H when step P fails.
R') Proceed as step R with X, Y interchanged.

Failure

It may happen that there is more than one solution to the equation. In this case, step Q will never reduce the set S of possible values to $\{0\}$, and step P will always fail. However, examination of the possible values in S will give information about the congruence classes of the further solutions (m, n) modulo p for the p in H and it should then be possible to use the Chinese Remainder Theorem and the Baker bounds to find the further solutions exactly. These can then be added to the known list and the process repeated with appropriate subsequences of the X and Y.

Failure

It will not be possible to carry out Step Q in order to add a prime p from H to the modulus N unless there is a prime q in L with the corresponding cycle length ℓ_χ divisible by p. For given p, it is not clear that there exists any such q. The existence of such q for sufficiently large p is guaranteed by a theorem of Stewart, although it should be noted that the lower bound for p in our applications would be of the order 10^{266}. However Stewart also shows that there are only finitely many sequences for which this lower bound cannot be taken to be 13.

Conclusions

We have presented a practical method for proving the completeness of a list of integral points on particular models of an elliptic curve.

The method has been applied to giving a complete list of elliptic curves over $\mathbb{Q}(\sqrt{5})$ with good reduction away from 2.

Questions?

Questions?