Six unlikely intersection problems in search of effectivity

P. Habegger, G. Jones, D. Masser

Departement Mathematik und Informatik
Fachbereich Mathematik
Universität Basel
CH-4051 Basel

Preprint No. 2015-28
September 2015

www.math.unibas.ch

SIX UNLIKELY INTERSECTION PROBLEMS IN SEARCH OF EFFECTIVITY

P. HABEGGER, G. JONES, AND D. MASSER

Abstract. We investigate four properties related to an elliptic curve E_t in Legendre form with parameter t: the curve E_t has complex multiplication, E_{-t} has complex multiplication, a point on E_t with abscissa 2 is of finite order, and t is a root of unity. Combining all pairs of properties leads to six problems on unlikely intersections. We solve these problems effectively and in certain cases also explicitly.

1. Introduction

For any $t \in \overline{\mathbf{Q}} \setminus \{0, 1\}$ we consider the elliptic curve E_t

$$y^2 = x(x-1)(x-t) \tag{1}$$

whose j-invariant equals

$$j = 2^8 \frac{(t^2-t+1)^3}{t^2(1-t)^2}. \tag{2}$$

We will investigate four properties of t.

The first is that E_t should have complex multiplication. The second, not a lot different, is that E_{-t} should have complex multiplication. The third is that the point $P_t = (2, \sqrt{4-2t})$ should be torsion on E_t. And the fourth is the simpler exponential analogue: t should be a root of unity.

It is well known that each property holds for infinitely many values of t. This is classical for the first two properties, was proved by Masser and Zannier in [22] for the third property, and is trivial for the fourth property.

We obtain six problems by looking at all pairs of properties. The reader is invited to imagine a regular tetrahedron with horizontal base whose vertices are the first, second, third properties, and whose apex is the fourth property. Thus the problems correspond to the six edges.

It is known that for any pair there are at most finitely many t having both properties. For the pair $\{1, 2\}$ of the first and second property, this reduces to a special case of the André-Oort conjecture for a certain plane curve (of degree 4), and this conjecture was proved by André [1] for all plane curves

For the pair $\{1, 3\}$ this is a special case of a result of André [2] when the complex multiplication order is maximal and in general by Pila [28].

For $\{1, 4\}$ the result is a very special case of Pila's result [29] (as indeed the results $\{1, 2\}, \{2, 4\}$ are as well).

The finiteness in $\{2, 3\}$ reduces to the point $(2, \sqrt{4+2t})$ on E_t and so the finiteness follows as in $\{1, 3\}$.

The finiteness in $\{2,4\}$ is equivalent to that in $\{1,4\}$ because $-t$ is a root of unity if and only if t is.

Finally, the finiteness in $\{3,4\}$ can be deduced from the result of Masser and Zannier [23] by taking complex conjugates to deduce that $\overline{P_t} = P_{\bar{t}} = P_{1/t} = (2, \sqrt{4-2/t})$ is torsion on $E_{1/t}$, and noting that $E_t, E_{1/t}$ are isomorphic to get another point $Q_t = (2t, t\sqrt{4t-2})$ on E_t. One must check that P_t, Q_t are generically linearly independent; but this follows easily from the fact that P_t is ramified only at $t = 2$ and Q_t only at $t = 1/2$.

All these proofs have various elements of possible ineffectivity which make it difficult or impossible actually to find the finite set in question. Thus in [1], [28], and [29] there is an appeal to Siegel-Brauer on class numbers, ineffective to this day. And in [2] results of Silverman on bounded height and Colmez on unbounded height are used, which involve unspecified constants. Finally in [23] (which also uses Silverman's result) a key role is played by Pila's estimates for rational points on analytic surfaces which involve sophisticated compactness results of Gabrielov.

Since these proofs, there has been some progress towards effectivity. Regarding our problem pairs, we now know the following.

For $\{1,2\}$ effective versions of André's Theorem [1] were proved independently by Kühne [16] and Bilu, Masser and Zannier [4]. The effectivity was illustrated by the line $x + y = 1$ and the hyperbola $xy = 1$; however our curve is much more complicated. We succeed here to show in Theorem 1 that there are no t with a bit of what looks like luck.

For $\{1,3\}$ we use a method involving supersingular primes and the Chebotarev Density Theorem. We show in Theorem 2 that the finite set consists exactly of $t = 2$ and the two roots of $t^2 - 16t + 16 = 0$.

For $\{1,4\}$ the effectivity follows from work of Paulin [27, 26], whose result even implies that the order of t is at most 2346. Here we show in Theorem 3 that $t = 1$ or $e^{\pm\pi i/3}$.

For $\{2,3\}$ we could hope to proceed as in $\{1,3\}$, but it is not clear if this works. Instead we return to the method of height comparison; we hope that our methods of calculating the constants may have other applications. Here we prove in Theorem 4 for example that $\frac{2^8(t^2+t+1)^3}{t^2(t+1)^2} = j(\tau)$ for the modular function, with $a\tau^2 + b\tau + c = 0$ for integers a, b, c satisfying

$$0 \le b \le a \le \sqrt{-D/3},\ b^2 - 4ac = -D$$

and $0 < -D < 2 \cdot 10^{32}$.

As mentioned above we can forget about $\{2,4\}$.

Finally for $\{3,4\}$ we use an idea of Boxall and Jones [6] involving transcendence measures to obtain a zero estimate which can then be fed into the Bombieri-Pila machinery on analytic curves (also not entirely luck-free). Here we show in Theorem 5 only that the order of t can be bounded in an effective way.

In connexion with the third property one must mention the surprising result of Stoll [33] that there are no complex numbers $t \neq 0, 1$ such that $(2, \sqrt{4-2t})$ and $(3, \sqrt{18-6t})$ are both torsion (the original unlikely intersection proposed in [22]).

One can also consult Wüstholz [37] for interesting discussions about the general topic of effectivity and in particular the problems of inverting the modular function.

2. E_t AND E_{-t} HAVE CM $\{1,2\}$

We consider the pair $\{1,2\}$. We prove the following.

Theorem 1. *There are no complex numbers $t \neq 0, 1, -1$ such that the elliptic curves E_t and E_{-t} both have complex multiplication.*

We note for comparison that E_t, E_{1-t} are isomorphic, so there are infinitely many t such that they both have complex multiplication.

Because the j-invariants are respectively

$$x = 256\frac{(t^2-t+1)^3}{t^2(1-t)^2}, \quad y = 256\frac{(t^2+t+1)^3}{t^2(1+t)^2} \tag{3}$$

which are related by

$$\begin{aligned} &x^3y - 2x^2y^2 + xy^3 - 1728x^3 + 1216x^2y + 1216xy^2 - 1728y^3 + 3538944x^2 \\ &\quad - 2752512xy + 3538944y^2 - 2415919104x - 2415919104y + 549755813888 = 0 \end{aligned} \tag{4}$$

this is implied by the fact that (4) has no solutions in singular moduli x, y; that is, values of the j-function $j(\tau)$ at quadratic numbers τ in the upper half plane.

Actually the two facts are equivalent, because (3) for $t \neq 0, 1, -1$ parametrizes the entire affine curve (4); i.e. there are no missing points. To see this we use the identity

$$F(R(t), y) = S(t)^2(y - R(-t))(y - R(-t'))(y - R(-t'')) \tag{5}$$

where $F(x, y)$ is the left-hand side of (4),

$$R(t) = 256\frac{(t^2-t+1)^3}{t^2(1-t)^2}$$

as in (3),

$$S(t) = 8\frac{(2t-1)(t-2)(t+1)}{t(1-t)},$$

and $t' = 1 - t$, $t'' = (t-1)/t$. For any point (x, y) on (4) we can write $x = R(t)$ for $t \neq 0, 1$. If $x = 1728 = R(1/2) = R(2) = R(-1)$ then $y = 21952/9 = R(-1/2)$, so we can assume $t \neq 1/2, 2, -1$. It now follows from (5) that y is one of $R(-t), R(-t'), R(-t'')$. But at the same time $R(t) = R(t') = R(t'')$.

André [1] determined when when there are only finitely many singular moduli x, y satisfying a given polynomial equation $\mathcal{F}(x, y) = 0$ and when not. His proof did not allow an effective determination of all solutions due to the use of the Siegel-Brauer Theorem. This ingredient was eliminated by Kühne [16] in 2012 and independently by Bilu, Masser and Zannier [4] in 2013 thus yielding effectivity. This was illustrated by a second paper [17] of Kühne showing that there are no solutions on the line $x + y = 1$. And in [4] it was also shown, with a bit more trouble, that there are no solutions on the hyperbola $xy = 1$.

At first sight it looks like (4), now our $F(x, y) = 0$, should be a lot more trouble. But happily it turns out that certain simplifying features for the line and the hyperbola persist for (4). In general the difficulty depends crucially on the points at infinity on the curve $\mathcal{F}(x, y) = 0$. For $x + y = 1$ there is only one, corresponding to the asymptote $y = -x$. A general $y = \alpha x$ would require the use of linear forms in two logarithms; but if α is a root of unity then we can get by with a single logarithm, which comes down

to a simple Liouville-type estimate for an algebraic number. For $xy = 1$ there is an asymptote $y = 0$. A general $y = \alpha$ would require the use of linear forms in two elliptic logarithms, with some resulting computational troubles; but if α happens itself to be a singular modulus then again we can get by with Liouville. As $0 = j((1+\sqrt{-3})/2)$ this is the case here, and there remain only minor ramification troubles in inverting $j(\tau)$ near $\tau = (1+\sqrt{-3})/2$ (which has a zero of order 3 there).

For (4) it is not absolutely obvious at first sight what happens near infinity. By symmetry we can assume x large. By (3) this implies t is near $0, 1, \infty$. Then y is near $\infty, 1728, \infty$ respectively. For the first of these x, y are both about $256/t^2$, so the asymptote is $y = x$. For the third x, y are both about $256t^2$, so again $y = x$. So no logarithms. As for the second, we see that x is about $256/(1-t)^2$ and y is about 1728, so the asymptote is $y = 1728$; and lo and behold $1728 = j(\sqrt{-1})$. So no elliptic logarithms either. But the ramification persists, now of order 2 rather than 3 above.

We start with a study of the rational function $R(t)$. It is well-known to be invariant under the group generated by the transformations taking t to $1/t$ and $1 - t$.

We can check that for real t it is monotonic on the six open intervals

$$(-\infty, -1),\ (-1, 0),\ (0, 1/2),\ (1/2, 1),\ (1, 2),\ (2, \infty). \tag{6}$$

(alternately decreasing and increasing) with local minima at $t_0 = -1, 1/2, 2$ when $R(t_0) = 1728$. Thus if $x > 1728$ then there are exactly six different real t with $R(t) = x$, one in each of the intervals (6); and there are no non-real t with $R(t) = x$. The next result specifies $y = R(-t)$ more precisely in each of the intervals when $x \geq 1000000$ (among other things).

Lemma 1. *Suppose* $R(t) \geq 1000000$.

(i) *If* $t < -1$ *then* $R(-t) \geq R(t) - 32\sqrt{R(t)}$.
(ii) *If* $-1 < t < 0$ *then* $R(-t) \geq R(t) - 32\sqrt{R(t)}$.
(iii) *If* $0 < t < 1/2$ *then* $R(-t) \geq R(t)$.
(iv) *If* $1/2 < t < 1$ *then* $R(t) \leq 265(t-1)^{-2}$ *and* $0 < R(-t) - 1728 \leq 1363(t-1)^2$.
(v) *If* $1 < t < 2$ *then* $R(t) \leq 270(t-1)^{-2}$ *and* $0 < R(-t) - 1728 \leq 1340(t-1)^2$.
(vi) *If* $t > 2$ *then* $R(-t) \geq R(t)$.

Proof. In (i) we must have $t \leq -60$, else $R(t) < R(-60) < 1000000$. We calculate

$$1024R(t) - (R(-t) - R(t))^2 = -262144\frac{P(t)}{t(t-1)^4(t+1)^4}$$

for a polynomial $P(t) = t^{10} + \cdots$ with no real zero $t \leq -60$. Thus $P(t) > 0$ for such t, and the result follows.

In (ii) we get the result immediately from (i) by replacing t by $1/t$.

In (iii) we have $t \leq 1/60$, else $R(t) < R(1/60) = R(60) < 1000000$. Now

$$R(-t) - R(t) = 512\frac{P(t)}{t(t-1)^2(t+1)^2}$$

for a polynomial $P(t)$ with $P(0) > 0$ and no positive real zero $t \leq 1/60$. Thus $P(t) > 0$ for such t, and the result follows.

In (iv) we have $t \geq 1 - 1/60$, else $R(t) < R(1 - 1/60) = R(60)$. Now

$$R(t) = R(1-t) = 256\frac{(1-(1-t)+(1-t)^2)^3}{t^2(1-t)^2} \leq 256\frac{1}{(1-1/60)^2(1-t)^2} < \frac{265}{(1-t)^2}$$

and

$$R(-t)-1728 = 64\frac{(t+2)^2(2t+1)^2(t-1)^2}{t^2(t+1)^2} < 5184\frac{(t-1)^2}{(1-1/60)^2(2-1/60)^2} < 1363(t-1)^2.$$

In (v) we have $t \leq 1 + 1/60$, else $R(t) < R(1 + 1/60) < 1000000$. Now

$$R(t) = 256\frac{(t^2-t+1)^3}{t^2(1-t)^2} \leq 256\frac{((1+1/60)^2-(1+1/60)+1)^3}{(1-t)^2} < \frac{270}{(1-t)^2}$$

and

$$R(-t)-1728 = 64\frac{(t+2)^2(2t+1)^2(t-1)^2}{t^2(t+1)^2} < 16(3+1/60)^2(3+1/30)^2(t-1)^2 < 1340(t-1)^2.$$

In (vi) we get the result immediately from (iii) using by replacing t by $1/t$.
This completes the proof. □

We will also have to solve $R(t) = x$ for $x < 1728$. Here there are no real solutions. If $x < 0$ there are still six different complex solutions, and they have real part $1/2$ or lie on the circles $|t| = 1$ and $|t - 1| = 1$. This can be seen from

$$R(1/2 + iv) = -64\frac{(4v^2-3)^3}{(4v^2+1)^2},$$

which is monotonic increasing on $(-\infty, 0)$, monotonic decreasing on $(0, \infty)$ and zero at $v = \pm\sqrt{3}/2$ (with graph looking a bit like a buddhist temple); thus there are solutions with $v > \sqrt{3}/2$ and $v < -\sqrt{3}/2$. And from

$$R(u + i\sqrt{1-u^2}) = 128\frac{(2u-1)^3}{u-1}$$

which is monotonic decreasing on $(-1, 1)$ (with each choice of sign for the square root) and zero at $u = 1/2$; so there are two solutions with $1/2 < u < 1$. And

$$R(1 + u + i\sqrt{1-u^2}) = 128\frac{(2u+1)^3}{u+1}$$

which is similarly monotonic increasing on $(-1, 1)$ and zero at $u = -1/2$; so there are two solutions with $-1 < u < -1/2$.

Lemma 2. *Suppose $R(t) \leq -190000$.*

(i) *If $t = 1/2 + iv$ with $v > \sqrt{3}/2$ then $|R(-t)| \geq -R(t)$.*
(ii) *If $t = 1/2 + iv$ with $v < -\sqrt{3}/2$ then $|R(-t)| \geq -R(t)$.*
(iii) *If $t = u + i\sqrt{1-u^2}$ with $u > 1/2$ and $\sqrt{1-u^2} > 0$ then $R(t) \geq -128(1-u)^{-1}$ and $-2593(1-u) \leq R(-t) - 1728 < 0$.*
(iv) *If $t = u + i\sqrt{1-u^2}$ with $u > 1/2$ and $\sqrt{1-u^2} < 0$ then $R(t) \geq -128(1-u)^{-1}$ and $-2593(1-u) \leq R(-t) - 1728 < 0$.*
(v) *If $t = 1 + u + i\sqrt{1-u^2}$ with $u < -1/2$ and $\sqrt{1-u^2} > 0$ then $|R(-t)| \geq -R(t)$.*
(vi) *If $t = 1 + u + i\sqrt{1-u^2}$ with $u < -1/2$ and $\sqrt{1-u^2} < 0$ then $|R(-t)| \geq -R(t)$.*

Proof. In (i), (ii) we find

$$|R(-t)|^2 - R(t)^2 = 32768\frac{P(v)}{(4v^2+1)^4(4v^2+9)^2}$$

for a polynomial $P(v)$ with non-negative coefficients, so the results are clear.

In (iii) we have $u \geq u_0 = 1 - 1/1450$, else $R(u + i\sqrt{1-u^2}) > R(u_0 + i\sqrt{1-u_0^2}) > -190000$. Now

$$-R(t) = 128\frac{(2u-1)^3}{1-u} \leq 128(1-u)^{-1}$$

and

$$1728 - R(-t) = 64\frac{(1-u)(5+4u)^2}{u+1} \leq 5184\frac{1-u}{u_0+1} \leq 2593(1-u).$$

Part (iv) follows by complex conjugation.

In (v), (vi) we have

$$|R(-t)|^2 - R(t)^2 = -65536\frac{P(u)}{(u+1)(4u+5)^2}$$

for a polynomial $P(u)$ with no real zeroes between -1 and $-1/2$ and $P(-3/4) < 0$, so the results follow.

□

Next comes the study of $j(\tau)$ itself.

Lemma 3. *If τ is in the standard fundamental domain with imaginary part y then $||j(\tau)| - e^{2\pi y}| \leq 2079$.*

Proof. This is Lemma 1 of [4]. It is essentially inversion of $j(\tau)$ near $\tau = \infty$. □

Now we have the crucial inversion near $\tau = i$, first only on the imaginary axis.

Lemma 4. *If $\tau = iy$ for $y \geq 1$ and $0 < j(\tau) - 1728 \leq \delta \leq 2$ then $0 < y - 1 \leq \sqrt{\delta}/150$.*

Proof. We note that $y \leq y_0 = 101/100$ else $j(\tau) > j(iy_0) > 1730$. Now for $f(y) = j(iy) = e^{2\pi y} + \cdots$ we have

$$f''(y) = (2\pi)^2 e^{2\pi y} + \sum_{n=1}^{\infty} c_n (2\pi n)^2 e^{-2\pi n y}$$

for $c_n \geq 0$. This is at least

$$(2\pi)^2 e^{2\pi} + \sum_{n=1}^{\infty} c_n (2\pi n)^2 e^{-2\pi n y_0} = (2\pi)^2 e^{2\pi} + f''(y_0) - (2\pi)^2 e^{2\pi y_0}.$$

A calculation shows that $f''(y_0) > 48364$ - it is most easily done using

$$\frac{d^2 j}{d\tau^2} = -1152\pi^2 \frac{E_4(4E_6^2 + 3E_4^3 - E_2 E_4 E_6)}{E_4^3 - E_6^2}$$

for the standard modular forms E_4, E_6 and the related E_2 (definitely not Legendre curves) Thus $f''(y) \geq 46993$. And now

$$\delta \geq j(\tau) - 1728 = f(y) - f(1) = \frac{1}{2} f''(\eta)(y-1)^2$$

for $1 < \eta < y$, and the result follows. □

And finally the inversion near $\tau = i$ on the unit circle.

Lemma 5. *If $\tau = e^{i\theta}$ for $\pi/3 \le \theta \le 2\pi/3$ and $-2 \le -\delta \le j(\tau) - 1728 \le 0$ then $|\theta - \pi/2| \le \sqrt{\delta}/100$.*

Proof. The analogous proof for $|j(\tau)| \le \delta$ in [4] was heavily geometrical, especially in Lemma 2, because we were working in the complex plane. Here we restrict to real analysis. After all, $f(\theta) = j(e^{i\theta})$ is real if θ is, thanks to

$$\overline{f(\theta)} = \overline{j(e^{i\theta})} = j(-e^{-i\theta}) = j(e^{i\theta}) = f(\theta).$$

As $j'(i) = 0$ the leading term in the power series of $j(e^{i\theta}) - 1728$ about $\theta = \pi/2$ involves f''. To evaluate this derivative we use again E_4, E_6 and E_2, for which the analogous quantities

$$e_4(\theta) = e^{2i\theta}E_4(e^{i\theta}), \quad e_6(\theta) = e^{3i\theta}E_6(e^{i\theta})$$

are also real. And adjusting $E_2(\tau)$ by $3/(\pi \mathrm{Im}(\tau))$ in the usual way we see too that

$$e_2(\theta) = e^{i\theta}\left(E_2(e^{i\theta}) - \frac{3}{\pi \sin\theta}\right)$$

is real.

We now start estimating (as if we had been doing something entirely different for the last five pages).

On the fundamental domain we have

$$|E_4(\tau)| \le 1 + 240\sum_{n=1}^{\infty}\sigma_3(n)e^{-n\pi\sqrt{3}} = C_4 = E_4\left(\frac{i\sqrt{3}}{2}\right)$$

and rather similarly

$$|E_6(\tau)| \le 1 + 504\sum_{n=1}^{\infty}\sigma_5(n)e^{-n\pi\sqrt{3}} = C_6 = 2 - E_6\left(\frac{i\sqrt{3}}{2}\right),$$

$$|E_2(\tau)| \le C_2 = 2 - E_2\left(\frac{i\sqrt{3}}{2}\right).$$

It follows that for $E_4' = 2\pi i(E_2E_4 - E_6)/3$ we have

$$|E_4'(\tau)| \le C_4' = 2\pi(C_2C_4 + C_6)/3,$$

for $E_6' = \pi i(E_2E_6 - E_4^2)$ that

$$|E_6'(\tau)| \le C_6' = \pi(C_2C_6 + C_4^2),$$

and for $E_2' = \pi i(E_2^2 - E_4)/6$ that

$$|E_2'(\tau)| \le C_2' = \pi(C_2^2 + C_4)/6.$$

So for real θ with $\pi/3 \le \theta \le 2\pi/3$ we deduce

$$|e_4'(\theta)| = |2ie^{2i\theta}E_4(e^{i\theta}) + ie^{3i\theta}E_4'(e^{i\theta})| \le c_4' = 2C_4 + C_4',$$

$$|e_6'(\theta)| \le c_6' = 3C_6 + C_6',$$

and for

$$e_2'(\theta) = ie^{i\theta}E_2(e^{i\theta}) + ie^{2i\theta}E_2'(e^{i\theta}) + \frac{3}{\pi \sin^2\theta}$$

we get

$$|e_2'(\theta)| \le c_2' = C_2 + C_2' + \frac{4}{\pi}.$$

A calculation yields

$$f'' = 3456\pi^2 e_4 - \frac{1152\pi e_4 e_6(3ce_4 + \pi s e_2 e_4 - 7\pi s e_6)}{s(e_4^3 - e_6^2)} \tag{7}$$

with $c = \cos\theta,\ s = \sin\theta$.

At $\theta = \pi/2$ we have the well-known values

$$e_2 = 0, \quad e_4 = -E_4(i) = -\frac{3\Gamma(1/4)^8}{(2\pi)^6}, \quad e_6 = 0. \tag{8}$$

Thus

$$f''\left(\frac{\pi}{2}\right) = 3456\pi^2 e_4 < -49655 \tag{9}$$

coming from the first term in (7). We show that the other terms in (7) are relatively small.

Now if $|f(\theta) - 1728| \le 2$ as in the present lemma, then by $f(\pi/2 + 1/100) < 1726$ and monotonicity (because $f \ne 0$ or equivalently $j \ne 0$) we deduce $|\theta - \pi/2| \le 1/100$. For such θ we have

$$\left|e_4(\theta) - e_4\left(\frac{\pi}{2}\right)\right| \le \frac{c_4'}{100}, \quad |e_6(\theta)| \le \frac{c_6'}{100}, \quad |e_2(\theta)| \le \frac{c_2'}{100} \tag{10}$$

and so from (9) we lose at most

$$3456\pi^2 \frac{c_4'}{100} < 5569. \tag{11}$$

For the other three terms in (7) we note first from (10) (see (8) also) that

$$|e_4(\theta)^3 - e_6(\theta)^2| \ge \left|\left|e_4\left(\frac{\pi}{2}\right)\right| - \frac{c_4'}{100}\right|^3 - \left(\frac{c_6'}{100}\right)^2 = \left(-e_4\left(\frac{\pi}{2}\right) - \frac{c_4'}{100}\right)^3 - \left(\frac{c_6'}{100}\right)^2 \ge 2.$$

The first of these terms, which is small because of e_6, can now be estimated by

$$\frac{1}{2}1152\pi C_4\left(3C_4\left(\frac{c_6'}{100}\right)\right)\Big/\sin\left(\frac{\pi}{2} + \frac{1}{100}\right) < 8537 \tag{12}$$

The second, which is small due to both e_2 and e_6, by

$$\frac{1}{2}1152\pi C_4\left(\pi\left(\frac{c_2'}{100}\right)\right) C_4\left(\frac{c_6'}{100}\right) < 368, \tag{13}$$

and the third, also doubly small, by

$$\frac{1}{2}1152\pi C_4\left(7\pi\left(\frac{c_6'}{100}\right)^2\right) < 10915, \tag{14}$$

a bit of a shock but fine.

We deduce from (9), (11), (12), (13), (14) that for $|\theta - \pi/2| \le 1/100$

$$|f''(\theta)| \ge 49655 - 5569 - 8537 - 368 - 10915 = 24266.$$

And finally

$$\delta \geq \left| f(\theta) - f\left(\frac{\pi}{2}\right)\right| = \frac{1}{2}|f''(\phi)| \left|\theta - \frac{\pi}{2}\right|^2 \geq \frac{1}{2} 24266 \left|\theta - \frac{\pi}{2}\right|^2$$

leading to the result. □

We can now tackle (4).

We write

$$x = j(\tau) = R(t), \quad y = j(\sigma) = R(-t)$$

with D, E as the respective discriminants of τ, σ. We can assume

$$|D| \geq |E|$$

and that τ, σ are in the fundamental domain, with

$$\sigma = \frac{b + \sqrt{E}}{2a}$$

so

$$|b| \leq a \leq \sqrt{\frac{|E|}{3}}.$$

There are two cases according to the parity of D.

First suppose D is even, $|D| \geq 20$. Then by conjugating we can assume $\tau = \sqrt{D}/2$. By Lemma 3

$$R(t) = j(\tau) = |j(\tau)| \geq e^{\pi\sqrt{|D|}} - 2079 \geq e^{\pi\sqrt{20}} - 2079 > 1000000.$$

Now t is real and Lemma 1 gives six subcases.

If $t < -1$ we get

$$y \geq e^{\pi\sqrt{|D|}} - 2079 - 32\sqrt{e^{\pi\sqrt{|D|}} - 2079}. \tag{15}$$

But if $a \neq 1$ or $E \neq D$ then again by Lemma 3

$$|y| = \left| j\left(\frac{b + \sqrt{E}}{2a}\right)\right| \leq e^{\pi\sqrt{|D|-1}} + 2079 < e^{\pi\sqrt{|D|}} e^{-\pi/(2\sqrt{|D|})} + 2079$$

a contradiction for $|D| \geq 20$ (and even $|D| \geq 15$).

Thus $\sigma = \frac{b+\sqrt{D}}{2}$ with $b = 0, 1$. If $b = 0$ then $y = x$. But

$$F(x, x) = -1024(x - 128)(x - 2048)^2$$

and neither 128 nor 2048 are singular moduli, cf. the complete list of rational singular moduli in Section 12.C. [7]. If $b = 1$ then $j(\sigma) = j(\tau + 1/2)$ so $\Phi_4(x, y) = 0$ for the modular transformation polynomial. Now the real roots $x > 1000000$ of the resultant of $F(x, y)$ and $\Phi_4(x, y)$ with respect to y are about

$$8.219997135 \cdot 10^{10}, \quad 8.225266165 \cdot 10^{10}.$$

These come nowhere near the $j(\sqrt{D}/2)$ for $|D| \geq 20$, apart from $D = -64$, where they are both are dangerously close to

$$j\left(\frac{\sqrt{-64}}{2}\right) = 41113158120 + 29071392966\sqrt{2} \approx 8.222631632 \cdot 10^{10}.$$

However the latter cannot be a zero of the resultant, because that has irreducible factors of degrees only 4,6,7.

If $-1 < t < 0$ we get the same lower bound for y as for $t < -1$ and so we can proceed as above.

If $0 < t < 1/2$ it is even better.

If $1/2 < t < 1$ then we get

$$0 < j(\sigma) - 1728 \le \frac{1363 \cdot 265}{e^{\pi\sqrt{|D|}} - 2079} < 1.$$

Now j is real only on the boundary of the fundamental domain or the part on the imaginary axis. And $j > 1728$ only on the latter. It follows from Lemma 4 that

$$0 < \frac{\sqrt{|E|}}{2a} - 1 < \frac{1}{150}\sqrt{\frac{1363 \cdot 265}{e^{\pi\sqrt{|D|}} - 2079}} < \frac{1}{150}.$$

Thus

$$0 < |E| - 4a^2 = 4a^2 \left(\frac{\sqrt{|E|}}{2a} - 1\right)\left(\frac{\sqrt{|E|}}{2a} + 1\right) < \frac{4|D|}{3}\frac{1}{150}\sqrt{\frac{1363 \cdot 265}{e^{\pi\sqrt{|D|}} - 2079}}\left(2 + \frac{1}{150}\right) < 1$$

for $|D| \ge 20$, which contradicts the Fundamental Theorem of Transcendence.

If $1 < t < 2$ it is much the same.

And if $t > 2$ it is the same as $0 < t < 1/2$.

This completes the case of even D, so we next assume D is odd, now $|D| \ge 15$. Then by conjugating we can assume $\tau = (1 + \sqrt{D})/2$. By Lemma 3

$$R(t) = j(\tau) = -|j(\tau)| \le -e^{\pi\sqrt{|D|}} + 2079 \le -e^{\pi\sqrt{15}} + 2079 < -190000.$$

Now t is non-real and Lemma 2 gives six more subcases, but up to complex conjugation only three.

If $t = 1/2 + iv$ with $v > \sqrt{3}/2$ then

$$|y| \ge e^{\pi\sqrt{|D|}} - 2079$$

and we can argue as in (15), even for $|D| \ge 15$ (now there are no real roots $x < -190000$ of the resultant).

If $t = u + i\sqrt{1 - u^2}$ with $u > 1/2$ and $\sqrt{1 - u^2} > 0$ then

$$-2 < -\frac{2593 \cdot 128}{e^{\pi\sqrt{|D|}} - 2079} < j(\sigma) - 1728 < 0.$$

Now σ must be on the boundary but not its vertical part: $\sigma = e^{i\theta}$ with $\pi/3 \le \theta \le 2\pi/3$ but $\theta \ne \pi/2$. Thus Lemma 5 gives

$$0 < \left|\theta - \frac{\pi}{2}\right| \le \frac{1}{100}\sqrt{\frac{2593 \cdot 128}{e^{\pi\sqrt{|D|}} - 2079}}.$$

So

$$0 < \left|\frac{\sqrt{|E|}}{2a} - 1\right| = |\sin\theta - 1| \le \frac{1}{2}\left|\theta - \frac{\pi}{2}\right|^2,$$

much better than before.

If $t = 1 + u + i\sqrt{1-u^2}$ with $u < -1/2$ and $\sqrt{1-u^2} > 0$ then it is pretty much the same as $t = 1/2 + iv$.

This finishes the largish discriminants.

If $|D| < 20$ is even then $-D = 4, 8, 12, 16$ and

$$x = 1728, 8000, 54000, 287496.$$

The first implies $y = 21952/9$ not a singular modulus because not an algebraic integer. The second implies $y = 10976$ not a singular modulus, or $49y^2 - 358528y + 481890304 = 0$ also not an algebraic integer. The third and fourth give no algebraic integers.

If $|D| < 15$ is odd then $-D = 3, 7, 11$ and

$$x = 0, -3375, -32768.$$

The first implies $y = 2048/3$ not an algebraic integer. The second and third give no algebraic integers.

This completes the proof of Theorem 1.

3. $(2, *)$ is torsion and E_t has CM $\{1, 3\}$

In this section we consider the pair $\{1, 3\}$. We prove the following

Theorem 2. *Suppose $t \in \overline{\mathbf{Q}} \smallsetminus \{0, 1\}$ such that E_t has complex multiplication. If $(2, *) \in E_t(\overline{\mathbf{Q}})$ has finite order n, then*

$$n = 2 \quad \textit{and} \quad t = 2$$

or

$$n = 6 \quad \textit{and} \quad t^2 - 16t + 16 = 0.$$

Conversely, if $n = 2$ or $n = 6$ then E_t has complex multiplication if t is a root of the corresponding polynomial.

Our method uses a variation on Parish's argument [25] to bound the number of rational torsion points on elliptic curves with complex multiplication.

Throughout this section we suppose that E_t has complex multiplication by an order in an imaginary quadratic number field K. The discriminant of K will be denoted by $\Delta_K < 0$. If will also be convenient to write $j \in \mathbf{Q}(t)$ for the j-invariant of E_t, it is given by (2).

Let us first treat the case where E_t has additional automorphisms.

Lemma 6. *If $t \neq 2$ and E_t has j-invariant 1728 or 0, then $(2, *)$ has infinite order.*

Proof. For $t \neq 2$, the order of $(2, *)$ does not divide 2 and we have

$$[2](2, *) = \left(-\frac{1}{8} \frac{(t-4)^2}{t-2}, * \right).$$

The j-invariant of E_t is 1728 if and only if $t \in \{-1, 1/2, 2\}$. It is 0 if and only if $t = \zeta^{\pm 1}$ with ζ a primitive sixth root of unity. Thus the abscissa of $[2](2, *)$ is

$$\begin{cases} \frac{25}{24} & : \text{if } t = -1, \\ \frac{49}{48} & : \text{if } t = 1/2, \text{ and} \\ \frac{15}{16} \pm \frac{\sqrt{-3}}{48} & : \text{if } t = \zeta^{\pm 1}. \end{cases}$$

We observe that the abscissa is never integral above 2 and above 3. By Theorem VII.3.4(a) [32] the point $[2](2,*)$ and hence $(2,*)$ has infinite order if $t=-1$ or $t=\zeta^{\pm 1}$. If $t=1/2$, the model determining E_t is not integral at 2. But it is integral in the coordinates $x'=4x$ and $y'=8y$. There the abscissa of $[2](2,*)$ is $49/12$ and therefore still non-integral above 2 and above 3. As before we conclude that $(2,*)$ has infinite order. □

We also use $E_{\bar{t}}$ to denote the elliptic curve defined over any field k of characteristic unequal to 2 given by the Legendre parameter $\bar{t}\in k\smallsetminus\{0,1\}$.

A place v of a number field F is an extension from $\mathbf{Q}$ to F of either the archimedean absolute value or a p-adic absolute value for some prime p. In the latter case we write $v\mid p$ and let k_v denote the residue field of v. We can and will identify places $v\mid p$ with prime ideals in the ring of integers of F containing p.

In the lemma below let $(\frac{\cdot}{\cdot})$ denote the Kronecker symbol.

Lemma 7. *Let $p\geq 3$ be a prime with $(\frac{\Delta_K}{p})=-1$ and suppose $v\mid p$ is a place of $K(t)$ with $|t|_v=|t-1|_v=|j|_v=|j-1728|_v=1$. We write $\bar{t}\in k_v\smallsetminus\{0,1\}$ for the reduction of t modulo v. Then $E_{\bar{t}}$ is a supersingular elliptic curve and $\bar{t}\in\mathbf{F}_{p^2}$. Moreover, there exists $\epsilon\in\{\pm 1\}$ such that*

$$E_{\bar{t}}(\mathbf{F}_{p^{2m}})\cong(\mathbf{Z}/|(\epsilon p)^m-1|\mathbf{Z})^2$$

for all integers $m\geq 1$.

Proof. First we claim that if $\overline{E}$ is a supersingular elliptic curve defined over $\mathbf{F}_{p^2}$ with $p\geq 3$ whose j-invariant is not among $\{0,1728\}$, then there exists $\epsilon\in\{\pm 1\}$ such that $\overline{E}(\mathbf{F}_{p^{2m}})\cong(\mathbf{Z}/|(\epsilon p)^m-1|\mathbf{Z})^2$ for all $m\geq 1$.

Let $[n]$ denote multiplication by n endomorphism of $\overline{E}$ for any $n\in\mathbf{Z}$. As $\overline{E}$ is supersingular, $[p]$ is a purely inseparable isogeny of height 2. By Proposition 5.4, Chapter 13 [14] there is an automorphism u of $\overline{E}$ such that $u[p]=\mathrm{Fr}_{p^2}$ is the Frobenius endomorphism of degree p^2 of $\overline{E}$. In other words, Fr_{p^2} raises the affine coordinates to the power p^2. By the hypothesis on the j-invariant of $\overline{E}$ Theorem 10.1, Chapter III [32] implies that the only automorphisms are ± 1. Therefore, $\mathrm{Fr}_{p^2}=[\epsilon p]$ for some $\epsilon\in\{\pm 1\}$. Our claim follows since $\overline{E}(\mathbf{F}_{p^{2m}})$ is the kernel of the separable isogeny $\mathrm{Fr}_{p^2}^m-[1]=[(\epsilon p)^m-1]$.

We apply this claim to $E_{\bar{t}}$, which is a well-defined elliptic curve since $|t|_v=|t-1|_v=1$ and $p\neq 2$. Recall that the endomorphism ring of E_t is an order in the imaginary quadratic field K. The prime p is inert in K, so p generates a prime ideal in the ring of integers of K. By Theorem 12, Chapter 13 [18], the elliptic curve $E_{\bar{t}}$ is supersingular. The j-invariant $\bar{j}$ of $E_{\bar{t}}$ does not lie in $\{0,1728\}$ by hypothesis. The lemma will follow once we can establish $\bar{t}\in\mathbf{F}_{p^2}$.

The fact that the Legendre parameter of a supersingular elliptic curve in characteristic $p\geq 3$ lies in $\mathbf{F}_{p^2}$ is well-known, see Dwork's note just after the proof of his Lemma 8.7 [10]. We give a self contained proof in our situation using the claim above. Indeed, by Deuring's Theorem, $\bar{j}$ lies in $\mathbf{F}_{p^2}$, cf. Theorem V.3.1 [32]. Thus $y^2+xy=x^3-36x/(\bar{j}-1728)-1/(\bar{j}-1728)$ determines an elliptic curve $\overline{E}$ over $\mathbf{F}_{p^2}$ with j-invariant $\bar{j}$. By our claim above in the case $m=1$ and since $\epsilon p-1\equiv 0 \pmod 2$ we see that all three points of order two of $\overline{E}$ are defined over $\mathbf{F}_{p^2}$. So $\bar{t}\in\mathbf{F}_{p^2}$. □

Lemma 8. *Let p and v be as in the previous lemma. Suppose that $j \notin \{0, 1728\}$ and that E_t contains a point of finite order $n \geq 2$ with $p \nmid n$ whose abscissa is a rational number with denominator coprime to p. Then*

$$p^2 \equiv 1 \pmod{n}.$$

Proof. We keep the notation from the proof of the previous lemma and suppose the point in question has abscissa $\xi \in \mathbf{Q}$.

By hypothesis, the reduction $\overline{\xi}$ of ξ modulo v is well-defined. We obtain a point on $E_{\overline{t}}$ whose ordinate $\overline{\eta}$ satisfies $\overline{\eta}^2 = \overline{\xi}(\overline{\xi} - 1)(\overline{\xi} - \overline{t})$. By the previous lemma we know that $\overline{t} \in \mathbf{F}_{p^2}$, so $\overline{\eta} \in \mathbf{F}_{p^4}$.

Now the order of the reduced point $(\overline{\xi}, \overline{\eta})$ equals n, the order of $(\xi, *)$, because n is coprime to the residue characteristic. The previous lemma applied to $m = 2$ yields $E_{\overline{t}}(\mathbf{F}_{p^4}) \cong (\mathbf{Z}/(p^2 - 1)\mathbf{Z})^2$ and so $n \mid p^2 - 1$, as desired. □

For any integer $n \geq 1$ we set

$$\mathcal{N}(n) = \{a \in (\mathbf{Z}/n\mathbf{Z})^\times : a^2 = 1\}.$$

In the next lemma we use Euler's totient function φ.

Lemma 9. *Suppose that $j \notin \{0, 1728\}$. If E_t contains a point of finite order $n \geq 2$ whose abscissa is a rational number, then*

$$\frac{1}{2}\varphi(n) < \#\mathcal{N}(n). \tag{16}$$

Proof. We fix a constant $C \geq 3n$, which may also depend on t and the point of finite order, with the following property. If p is a prime with $p \geq C$ and v is any place of $K(t)$ above p, then $|t|_v = |t - 1|_v = |j|_v = |j - 1728|_v = 1$ and p does not divide the denominator of the abscissa from the assertion. Any prime p in

$$\mathcal{P}_1 = \left\{ p \text{ is a prime} : p \geq C \text{ and } \left(\frac{\Delta_K}{p}\right) = -1 \right\}.$$

satisfies the hypothesis of Lemma 8. Therefore, p lies in

$$\mathcal{P}_2 = \left\{ p \text{ is a prime} : p^2 \equiv 1 \pmod{n} \right\}.$$

In other words, we have $\mathcal{P}_1 \subset \mathcal{P}_2$.

We will now extract a weak form of the lemma by comparing the density of these two sets. Indeed, by Chebotarev's Density Theorem we have

$$\#\{p \in \mathcal{P}_1 : \ p \leq T\} = \frac{1}{2}\frac{T}{\log T} + o\left(\frac{T}{\log T}\right).$$

as $T \to \infty$. The same theorem tells us that primes are equidistributed among the $\varphi(n)$ residues in $(\mathbf{Z}/n\mathbf{Z})^\times$. Thus

$$\#\{p \in \mathcal{P}_2 : \ p \leq T\} = \frac{\#\mathcal{N}(n)}{\varphi(n)}\frac{T}{\log T} + o\left(\frac{T}{\log T}\right)$$

as $T \to +\infty$. As the density of primes in $\mathcal{P}_1$ is at most the density of primes in $\mathcal{P}_2$ we conclude

$$\frac{1}{2}\varphi(n) \leq \#\mathcal{N}(n).$$

It remains to show that strict inequality holds. It is this apparently minor strengthening that makes the verification below harmless on current computer hardware. We will assume $\varphi(n)/2 = \#\mathcal{N}(n)$ and deriving a contradiction.

Suppose there is a prime $p \geq C$ with $\left(\frac{\Delta_K}{p}\right) = 1$ with residue in $\mathcal{N}(n)$. If p' is a further prime with $p' \equiv p \pmod{n\Delta_K}$, then

$$\left(\frac{\Delta_K}{p'}\right) = \left(\frac{\Delta_K}{p}\right) = 1 \text{ and } p' \text{ has residue in } \mathcal{N}(n)$$

as $\left(\frac{\Delta_K}{\cdot}\right)$ has period $|\Delta_K|$. But the original p is coprime to $n\Delta_K$ so the set

$$\mathcal{P}_1' = \{p' \text{ is a prime} : p' \equiv p \pmod{n\Delta_K}\}$$

has positive density $1/\varphi(n|\Delta_K|)$. It is disjoint from $\mathcal{P}_1$, so $\mathcal{P}_1 \cup \mathcal{P}_1' \subset \mathcal{P}_2$ contradicts the fact that $\mathcal{P}_1$ and $\mathcal{P}_2$ have equal density $1/2$.

We have established that any sufficiently large prime p with $\left(\frac{\Delta_K}{p}\right) = 1$ satisfies $p^2 \not\equiv 1 \pmod{n}$. On the other hand, there exist infinitely many primes p with $p \equiv 1 \pmod{n\Delta_K}$. Each such prime satisfies $p \equiv 1 \pmod{\Delta_K}$, so $\left(\frac{\Delta_K}{p}\right) = 1$, and $p \equiv 1 \pmod{n}$, so $p^2 \equiv 1 \pmod{n}$. This is a contradiction. □

The inequality in the previous lemma imposes a strong restriction on n.

Lemma 10. *If $n \geq 2$ is an integer with $\varphi(n)/2 < \#\mathcal{N}(n)$, then $n \mid 24$.*

Proof. By the Chinese Remainder Theorem we find $\#\mathcal{N}(nn') = \#\mathcal{N}(n)\#\mathcal{N}(n')$ if n and n' are coprime integers. We factor $n = \ell_1^{e_1} \cdots \ell_g^{e_g}$ into pairwise distinct primes ℓ_i with exponents $e_i \geq 1$ and find

$$\prod_{i=1}^{g} \frac{\ell_i^{e_i-1}(\ell_i - 1)}{\#\mathcal{N}(\ell_i^{e_i})} = \frac{\varphi(n)}{\#\mathcal{N}(n)} < 2.$$

Each factor on the left is at least 1 since $\mathcal{N}(\ell_i^{e_i})$ is a subset of $(\mathbf{Z}/\ell_i^{e_i}\mathbf{Z})^\times$. So if $\ell = \ell_i$ and $e = e_i$ for some $1 \leq i \leq g$, then

$$\ell^{e-1}(\ell - 1) < 2\#\mathcal{N}(\ell^e).$$

We now bound $\#\mathcal{N}(\ell^e)$ from above to find a restriction on ℓ^e.

First suppose $\ell \geq 3$. The group $(\mathbf{Z}/\ell^e\mathbf{Z})^\times$ is cyclic and therefore there are at most two solutions of $a^2 = 1$ in $(\mathbf{Z}/\ell^e\mathbf{Z})^\times$. Thus $\ell^{e-1}(\ell - 1) < 4$ which implies $\ell = 3$. We find $\ell^{e-1} < 2$ and hence $e = 1$.

Now suppose $\ell = 2$ and $e \geq 2$. The group $(\mathbf{Z}/2^e\mathbf{Z})^\times$ is isomorphic to $(\mathbf{Z}/2\mathbf{Z}) \times (\mathbf{Z}/2^{e-2}\mathbf{Z})$. This leaves us with at most 4 possibilities for $a \in (\mathbf{Z}/2^e\mathbf{Z})^\times$ with $a^2 = 1$. As in the last paragraph we find $2^{e-1} < 8$ and thus $e \leq 3$.

The two previous paragraphs together imply $n \mid 2^3 \cdot 3 = 24$. □

Note that $\varphi(120)/2 = 16$ which equals $\#\mathcal{N}(120)$. So the strict inequality in Lemma 9 saves us from having to deal with a point of order 120.

We combine the conclusion of Lemma 9 with the one of the previous lemma and Lemma 6 to get the following statement. If an elliptic curve in Legendre form with complex multiplication and j-invariant not among $\{0, 1728\}$ contains a point of finite order $n \geq 2$ whose abscissa is rational, then $n \mid 24$. It would be interesting to have an

explicit description of all t such that E_t has complex multiplication and contains a point of finite order > 2 with rational abscissa.

To prove Theorem 2 we handle the case where the abscissa is 2.

Proof of Theorem 2. Say E_t has complex multiplication and $(2, *)$ has finite order $n \geq 2$. Observe that E_2 has j-invariant 1728 and complex multiplication by $\mathbf{Z}[\sqrt{-1}]$, moreover $(2, 0)$ has order 2 on this curve. This corresponds to $t = 2$ and $n = 2$. So let us assume $t \neq 2$, by Lemma 6 we may assume that the j-invariant of E_t is not among $\{0, 1728\}$.

We have $B_n(2, t) = 0$ for the denominator of $B_n(x, t)$ of abscissa of the multiplication by n map for some $n \mid 24$.

Using `pari/gp` we compute the polynomials B_n for n up to 24 and substitute 2 for x. We thus obtain polynomials in t, one for each n, with rational coefficients. We proceed by factoring these polynomials over the rationals. Thus we obtain potential minimal polynomials with integer coefficients of candidate legendre parameters. We will now eliminate most of these polynomials using classical properties of singular moduli.

The j-invariant of E_t is an algebraic integer. If v is a finite place $\mathbf{Q}(t)$ with $v \nmid 2$, then using the ultrametric triangle inequality together with (2) we get $|t|_v = 1$. As $t-1$ determines the same elliptic curve as E_t up to isomorphism we also get $|t-1|_v = 1$. Thus we eliminate all minimal polynomials constructed before where the leading or constant coefficient is not a power of 2.

Next we take those polynomials that survive and compute their resultant with $jt^2(t-1)^2 - 2^8(t^2-t+1)^3$ taken as a polynomial in t and coefficients in $\mathbf{Z}[j]$. We thus eliminate t and obtain candidate minimal polynomials for the j-invariant after factorizing in the polynomial ring over the integers. From these factors we remove those that are non-monic. So the j-invariant j of E_t is a root of one of the irreducible polynomials

$$\begin{aligned} &J - 1728, \\ &J - 54000, \\ &J^2 - 1230272J + 1783774976 \end{aligned} \tag{17}$$

where we have omitted a fourth irreducible polynomial (of degree 16 which has a coefficient greater than 10^{73}) whose reduction modulo 5 splits into distinct irreducible factors over $\mathbf{F}_5$ as follows

$$(J^2+3J+4)(J^3+4J^2+4J+2)(J^{11}+3J^{10}+2J^9+3J^8+2J^7+3J^6+J^4+3J^3+2J^2+4J+3).$$

If j is a root of this fourth polynomial, then 5 splits into a product of three prime ideals in the ring of integers in $\mathbf{Q}(j)$. The residue degrees are $2, 3$, and 11. The extension $K(j)/\mathbf{Q}$ is Galois by Lemma 9.3 and Theorem 11.1 [7]. Thus the quotient of two residue degrees in $\mathbf{Q}(j)$ above 5 is $1/2, 1$, or 2. So we can exclude this fourth polynomial.

We have already treated the case $j = 1728$ at the beginning of this proof. To eliminate the two remaining polynomials we will proceed as follows.

In fact, 54000 is the j-invariant of the elliptic curve E_t with

$$(t^2 - 16t + 16)(t^2 + 14t + 1)(16t^2 - 16t + 1) = 0.$$

One checks readily that the point $(2, *)$ has finite order 6 if $t^2 - 16t + 16 = 0$, this is consistent with the statement of our theorem .

If $t^2+14t+1=0$ then we claim that $(2,*)$ does not have finite order. Indeed, in this case $t=-7\pm 4\sqrt{3}$ and we compute

$$[2](2,*)=\left(\frac{155}{88}\mp\frac{29}{66}\sqrt{3},*\right).$$

The abscissa of $[2](2,*)$ is not integral above 2 and above 3. So $[2](2,*)$ has infinite order.

If $16t^2-16t+1=0$, then we can argument similarly, in this case $t=1/2\pm\sqrt{3}/4$ and $[2](2,*)=(185/176\pm 31\sqrt{3}/1056,*)$ is not integral at a place above 11 and above 3 and therefore of infinite order.

We complete the proof by ruling out that a root j of (17) is the j-invariant of an elliptic curve with complex multiplication. Let us consider the elliptic curve E given by $y^2+xy=x^3-36x/(j-1728)-1/(j-1728)$; its j-invariant is just j. The polynomial (17) splits in $\mathbf{Q}(\sqrt{5})$ and has a root modulo 11 represented by 2. The curve E has good reduction at the place of $\mathbf{Q}(\sqrt{5})$ above 11 that corresponds to 2. The reduced curve is defined over $\mathbf{F}_{11}$ and the trace of its Frobenius is 4. So the reduced curve is ordinary. Its endomorphismus algebra is the imaginary quadratic field $\mathbf{Q}(\sqrt{-7})$ as $4^2-4\cdot 11=-28$. We repeat the same compution with $p=19$; modulo 19 we find that (17) has two distinct roots, one is represented by -2. This time the reduced elliptic curve over $\mathbf{F}_{19}$ has trace of Frobenius -4. Its endormorphism algebra is $\mathbf{Q}(\sqrt{-15})$. Recall that reducing an elliptic curve induces an injection of the corresponding endomorphism rings. As $\mathbf{Q}(\sqrt{-7})\cap\mathbf{Q}(\sqrt{-15})=\mathbf{Q}$ we conclude that any root of (17) determines an elliptic curve without complex multiplication. □

4. E_t has CM and t is a root of unity $\{1,4\}$

In this section we consider the pair $\{1,4\}$, and show the following.

Theorem 3. *Suppose $t\in\overline{\mathbf{Q}}\smallsetminus\{-1,0,1\}$ such that E_t has complex multiplication. If t is a root of unity, then $t=-1$ or $t=e^{\pm\pi i/3}$. Conversely, if $t=-1$ or $t=e^{\pm\pi i/3}$, then E_t has complex multiplication.*

The second statement is easy. Indeed, the elliptic curve E_{-1} has complex multiplication by the Gaussian integers. If t has order 6, then E_t has j-invariant 0 by (2) and thus has complex multiplication by the ring of Eisenstein integers.

So let us assume that the order m of t is not in $\{1,2,6\}$. We suppose that E_t has complex multiplication and eventually derive a contradiction. The endomorphism ring of E_t is an order in an imaginary quadratic number field K. By (2), the j-invariant of E_t is $j=J(t)\in\overline{\mathbf{Q}}$ where J is the rational function $J(x)=2^8(x^2-x+1)^3x^{-2}(1-x)^{-2}$.

Lemma 11. *The function $f:(0,1)\to\mathbf{C}$ given by $f(\theta)=J(e^{2\pi i\theta})$ is real-valued, satisfies $f(\theta)=f(1-\theta)$, and the fiber $f^{-1}(f(\theta))$ contains 2 elements if $\theta\neq 1/2$.*

Proof. The first 2 claims follow from $\overline{f(\theta)}=J(\overline{e^{2\pi i\theta}})=J(e^{-2\pi i\theta})=J(e^{2\pi i\theta})=f(\theta)$ where we used $J(x)=J(x^{-1})$. It is well-known that if $x\in\mathbf{C}\smallsetminus\{0,1\}$, then the fiber of J through x is $\{x,1/x,1-x,1/(1-x),x/(x-1),(x-1)/x\}$. Say x lies on the unit circle and $1-x$ does not. Then the fiber of J restricted to the unit circle containing x contains only x and $1/x$. These are distinct if $x\neq\pm 1$. If x and $1-x$ both lie on the

unit circle, then $x = e^{\pm \pi i/3}$. Here too the fiber of J containing x consists only of x and $1/x$. □

Each conjugate of j over $\mathbf{Q}$ is of the form $f(k/m)$ for some integer $1 \leq k \leq m-1$ that is coprime to m. So j is totally real by the previous lemma. Since $m \neq 2k$ we also find that j has half as many conjugates as t. Thus $[\mathbf{Q}(j) : \mathbf{Q}] = [\mathbf{Q}(t) : \mathbf{Q}]/2$ and so $[\mathbf{Q}(t) : \mathbf{Q}(j)] = 2$.

Lemma 12. *The order m divides* 240.

Proof. As we have seen in the previous section, the extension $K(j)/\mathbf{Q}$ is Galois. But Lemma 9.3 and Theorem 11.1 [7] even tell us that its Galois group is isomorphic to $\mathrm{Gal}(K(j)/K) \rtimes \mathbf{Z}/2\mathbf{Z}$ where the non-trivial element in $\mathbf{Z}/2\mathbf{Z}$ acts by inversion on $\mathrm{Gal}(K(j)/K)$.

We split-up into two cases.

In the first case we assume that $K \subset \mathbf{Q}(t)$. Then $K(t)/\mathbf{Q}$ is an abelian extension whose Galois group is isomorphic to the unit group $(\mathbf{Z}/m\mathbf{Z})^\times$. In particular, $K(j)/\mathbf{Q}$ is abelian. The action of $\mathbf{Z}/2\mathbf{Z}$ described above implies that $ex(\mathrm{Gal}(K(j)/K))$ divides 2 where $ex(G)$ denotes the exponent of an abelian group G.

It seems that we are dangerously close to the notorious and unsolved problem of explicitly determining imaginary quadratic number fields whose class group have exponent 2. Of such, 65 are known classically. Weinberger [36] proved that there is at most additional example. Luckily, we can exploit the structure of $\mathrm{Gal}(\mathbf{Q}(t)/\mathbf{Q})$ to bypass these issues of ineffectivity.

We recall $[K(t) : \mathbf{Q}(j)] = [\mathbf{Q}(t) : \mathbf{Q}(j)] = 2$ and $[K(j) : \mathbf{Q}(j)] = 2$ since j is totally real. So $K(j) = K(t)$ and therefore $ex(\mathrm{Gal}(K(t)/K))$ divides 2. The Galois group of $K(t)/K$ is isomorphic to an index 2 subgroup of $(\mathbf{Z}/m\mathbf{Z})^\times$. Hence $ex((\mathbf{Z}/m\mathbf{Z})^\times)$ divides 4.

The second case is when $K \not\subset \mathbf{Q}(t)$, but the argument is similar. By Galois Theory we find that $K(t)/\mathbf{Q}$ is Galois with group $\mathrm{Gal}(\mathbf{Q}(t)/\mathbf{Q}) \times \mathrm{Gal}(K/\mathbf{Q}) \cong (\mathbf{Z}/m\mathbf{Z})^\times \times \mathbf{Z}/2\mathbf{Z}$. Thus $\mathrm{Gal}(K(t)/K)$ is isomorphic to $(\mathbf{Z}/m\mathbf{Z})^\times$. As in the first case, the extension $K(j)/\mathbf{Q}$ is abelian and we find that $\mathrm{Gal}(K(j)/K)$ has exponent dividing 2. We recall that $\mathbf{Q}(t)/\mathbf{Q}(j)$ is quadratic, and in particular Galois. Thus $K(t)/K(j)$ has the same degree as $\mathbf{Q}(t)/\mathbf{Q}(t) \cap K(j)$, which is at most 2. Again we find that $ex(\mathrm{Gal}(K(t)/K)) = ex((\mathbf{Z}/m\mathbf{Z})^\times)$ divides 4.

In both cases we have

$$ex((\mathbf{Z}/m\mathbf{Z})^\times) \mid 4 \tag{18}$$

which implies the assertion as follows. Let us abbreviate $e \geq 0$ for the largest power of 2 dividing m and write $m = 2^e \ell_1^{e_1} \cdots \ell_g^{e_g}$ with $\ell_1, \ldots, \ell_g$ odd, distinct prime divisors of m. By the Chinese Remainder Theorem we have

$$(\mathbf{Z}/m\mathbf{Z})^\times = (\mathbf{Z}/2^e\mathbf{Z})^\times \times \prod_i (\mathbf{Z}/\ell_i^{e_i}\mathbf{Z})^\times.$$

As in Section 3, each unit group $(\mathbf{Z}/\ell_i^{e_i}\mathbf{Z})^\times$ is cycle of order $\ell_i^{e_i-1}(\ell_i - 1)$ since each ℓ_i is odd. The remaining factor satisfies

$$(\mathbf{Z}/2^e\mathbf{Z})^\times \cong \begin{cases} 0 & : \text{if } e \leq 1, \\ \mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2^{e-2}\mathbf{Z} & : \text{if } e \geq 2. \end{cases}$$

Now we use (18) to restrict m as follows. For any i we have $(\ell_i - 1) \mid 4$. So the only possible odd prime divisors of m are 3 and 5. Their respective squares cannot divide m. Finally, we must have $e - 2 \leq 2$. So $e \leq 4$ which implies $m \mid 2^4 \cdot 3 \cdot 5 = 240$. □

Proof of Theorem 3. The divisors of 240 are

$$1, 2, 3, 4, 5, 6, 8, 10, 12, 15, 16, 20, 24, 30, 40, 48, 60, 80, 120, 240. \tag{19}$$

Let us suppose that m is a power of an odd prime p. Then $|1 - t|_v < 1$ for any place v of $\mathbf{Q}(t)$ above p. From this we easily deduce $|j|_p > 1$ using (2). This contradicts the well-known fact that j is an algebraic integer. This argument eliminates $m = 3$ and $m = 5$ but fails to cover other values.

What happens if $m = 4$? Then $t^2 = -1$ and $J(t) = 2^7$. Again, this is not a singular moduli.

We will now eliminate $m = 8$ using a method that works for the other divisors as well.

Suppose t has precise order 8. We start out by picking the auxiliary prime $p = 17$. Since $p \equiv 1 \pmod 8$ it splits completely in the cyclotomic field $\mathbf{Q}(t)$. The integers 2 and 8 represent elements $\overline{2}$ and $t_2 = \overline{8}$ in $\mathbf{F}_{17}$ whose multiplicative order are both 8. So there are two places $v_{1,2} \mid 17$ such that t modulo v_1 is $\overline{2}$ and t modulo v_2 is $\overline{8}$. We use these residues to construct two possible reductions of E_t in characteristic 17 as Legendre elliptic curves. The following table lists the Legendre equations, the trace of Frobenius, and the discriminant of the imaginary quadratic number field generated by a root of the said characteristic polynomial.

Legendre curve over $\mathbf{F}_{17}$	trace of Frobenius	field discriminant
$y^2 = x(x - \overline{1})(x - \overline{2})$	2	-4
$y^2 = x(x - \overline{1})(x - \overline{8})$	-6	-8

Observe that none of the reduced curves is supersingular as the trace of Frobenius is never divisible by 17. Thus the endomorphism rings of the reduced curves are orders in an imaginary quadratic field whose discriminant is given by the column on the right.

The endomorphism ring of E_t injects into the endomorphism ring of any of its reductions. As we are assuming that E_t has complex multiplication, the table above leads to a contradiction.

For each remaining m from (19) we provide an auxiliary prime p satisfying $p \equiv 1 \pmod m$, two elements $t_1, t_2 \in \mathbf{F}_p$ of multiplicative order m that serve as the Legendre parameter for ordinary elliptic curves, the trace of Frobenius $a_{1,2}$ for each reduction, and the discriminants of corresponding endomorphism algebras $\Delta_{1,2}$.

m	p	t_1	t_2	a_1	a_2	Δ_1	Δ_2
10	11	$\overline{2}$	$\overline{7}$	0	-4	-11	-7
12	13	$\overline{2}$	$\overline{6}$	6	2	-4	-3
15	31	$\overline{7}$	$\overline{14}$	8	0	-15	-31
16	17	$\overline{3}$	$\overline{5}$	-6	2	-8	-4
20	41	$\overline{2}$	$\overline{5}$	10	-6	-4	-8
24	73	$\overline{7}$	$\overline{17}$	2	-6	-8	-4
30	31	$\overline{3}$	$\overline{12}$	-4	0	-3	-31

m	p	t_1	t_2	a_1	a_2	Δ_1	Δ_2
40	41	$\overline{6}$	$\overline{11}$	2	-6	-40	-8
48	97	$\overline{2}$	$\overline{3}$	18	-14	-4	-3
60	61	$\overline{2}$	$\overline{6}$	-10	-2	-4	-15
80	241	$\overline{17}$	$\overline{21}$	18	-22	-40	-120
120	241	$\overline{3}$	$\overline{12}$	-14	-22	-3	-120
240	241	$\overline{7}$	$\overline{13}$	-30	26	-4	-8

For given m in the table, the two listed field discriminants are different. By the same argument as above this means that E_t does not have complex multiplication if t has order m. □

5. $(2,*)$ is torsion and E_{-t} has CM $\{2,3\}$

We consider the pair $\{2,3\}$ and prove the following.

Theorem 4. *Suppose $t \in \overline{\mathbf{Q}} \smallsetminus \{0,1\}$ such that E_{-t} has complex multiplication. If $(2,*) \in E_t(\overline{\mathbf{Q}})$ has finite order $n \geq 2$, then $n \leq 10^{10^{19}}$ and the discriminant of the ring of endomorphisms of E_{-t} is strictly less than $2 \cdot 10^{32}$ in modulus.*

The proof splits into two parts.

In this section we need to work with the absolute logarithmic Weil height $h(x)$ of an algebraic number x. We refer to Chapter 1 [5] for the definition and basic properties.

5.1. Bounding the height of t from above.

Lemma 13. *Let A, B be polynomials in $\mathbf{Z}[X]$ with $\max\{\deg A, \deg B\} = d \geq 1$, and suppose there exist $P_0, Q_0, P_\infty, Q_\infty$ in $\mathbf{Z}[X]$ with degrees at most $d-1$ and $r \neq 0$ in $\mathbf{Z}$ such that*

$$P_0(X)A(X) + Q_0(X)B(X) = r, \;\; P_\infty(X)A(X) + Q_\infty(X)B(X) = rX^{2d-1}.$$

Then for any algebraic x with $B(x) \neq 0$ we have

$$h\left(\frac{A(x)}{B(x)}\right) \geq dh(x) - \log C$$

where

$$C = \max\{L(P_0) + L(Q_0), L(P_\infty) + L(Q_\infty)\}$$

for the lengths.

Proof. Let K be a number field containing x. For any non-archimedean place $|\cdot|$ on K it is clear that

$$|rx^{2d-1}| = |P_\infty(x)A(x) + Q_\infty(x)B(x)| \leq \max\{1, |x|^{d-1}\} \max\{|A(x)|, |B(x)|\}. \tag{20}$$

We also have

$$|r| = |P_0(x)A(x) + Q_0(x)B(x)| \leq \max\{1, |x|^{d-1}\} \max\{|A(x)|, |B(x)|\}, \tag{21}$$

and so

$$|r| \max\{1, |x|^{2d-1}\} \leq \max\{1, |x|^{d-1}\} \max\{|A(x)|, |B(x)|\} \tag{22}$$

with the obvious cancellation. But for an archimedean place $|\cdot|$ of K we get an extra $L(P_\infty)+L(Q_\infty)\le C$ on the far right of (20), and an extra $L(P_0)+L(Q_0)\le C$ on the far right of (21). Thus an extra C on the far right of (22). Taking the product over all places and then the logarithm we get the desired result. □

Note that the upper bound

$$h\left(\frac{A(x)}{B(x)}\right)\le dh(x)+\log\max\{L(A),L(B)\}$$

is practically obvious.

Now considering $3P_t$ and using a Zimmer constant (see below) coming from the Weierstrass model we already get $h(t)<75$. But it is more efficient to calculate directly a Zimmer constant on the Legendre model.

This time working over $\mathbf{Z}[t]$ not $\mathbf{Z}$ we use

$$A(X,t)=X^4-2tX^2+t^2=(X^2-t)^2,\ B(X,t)=4X(X-1)(X-t)$$

(coming from the duplication formula) with

$$\begin{aligned}P_0(X,t)&=-12X^2+(8t+8)X+4t^2-8t+4,\\ Q_0(X,t)&=3X^3+(t+1)X^2-5tX-2t^2-2t,\\ P_\infty(X,t)&=4t^2(t^2-2t+1)X^3+2t^2(4t^2+4t)X^2-12t^4X,\\ Q_\infty(X,t)&=-2t^3(t+1)X^3-5t^4X^2+(t^5+t^4)X+3t^5.\end{aligned}$$

We have

$$P_0(X,t)A(X,t)+Q_0(X,t)B(X,t)=r,\ P_\infty(X,t)A(X,t)+Q_\infty(X,t)B(X,t)=rX^7$$

with $r=4t^2(t-1)^2$.

For non-archimedean we get

(23)
$$|rx^7|=|P_\infty(x,t)A(x,t)+Q_\infty(x,t)B(x,t)|\le\max\{1,|x|^3\}\max\{1,|t|^5\}\max\{|A(x,t)|,|B(x,t)|\}.$$

We also have

(24)
$$|r|=|P_0(x,t)A(x,t)+Q_0(x,t)B(x,t)|\le\max\{1,|x|^3\}\max\{1,|t|^5\}\max\{|A(x,t)|,|B(x,t)|\},$$

and so

$$|r|\max\{1,|x|^7\}\le\max\{1,|x|^3\}\max\{1,|t|^5\}\max\{|A(x,t)|,|B(x,t)|\}\tag{25}$$

with the obvious cancellation. But for an archimedean place we get an extra $L(P_\infty)+L(Q_\infty)\le 44+14=58$ on the far right of (23), and an extra $L(P_0)+L(Q_0)\le 44+14=58$ on the far right of (24). Thus an extra 58 on the far right of (25). Taking the product over all places and then the logarithm we get

$$h(2P)\ge 4h(P)-5h(t)-\log 58$$

for any P in $E_t(\overline{\mathbf{Q}})$, where the height is that of the abscissa. A much better upper bound holds, and we deduce the Zimmer-type bound

$$|h(P)-\hat{h}(P)|\le\frac{1}{3}(5h(t)+\log 58)\tag{26}$$

for the corresponding Néron-Tate height.

We now use $4P_t$. We find that this is $A_4(t)/B_4(t)$ with A_4 of degree 8 and B_4 of degree 7 both in $\mathbf{Z}[X]$. So $d = 8$ in Lemma 13. We find $P_0, Q_0, P_\infty, Q_\infty$ with $r = 2^{33}$ and $C = 192475067056128$; these are surprisingly small because large powers of 2 can be cancelled (the resultant of A_4, B_4 is -2^{160}). Thus $h(4P_t) \geq 8h(t) - \log C$. On the other this is at most $\frac{1}{3}(5h(t) + \log 58)$. Comparison gives

$$h(t) \leq 5.4070213804731854624. \tag{27}$$

Here are the explicit expressions, if it helps at all. First

$$A_4 = -X^8 + 160X^7 - 7104X^6 + 57344X^5 - 206336X^4 + 401408X^3 - 442368X^2 + 262144X - 65536,$$

$$B_4 = 288X^7 - 3648X^6 + 17408X^5 - 38912X^4 + 40960X^3 - 16384X^2.$$

Then

$$P_0 = 9486432X^6 - 110727168X^5 + 464270080X^4 - 827747840X^3 + 540543488X^2 + 524288X + 131072,$$

$$Q_0 = 32939X^7 - 5237482X^6 + 228793380X^5 - 1661849512X^4 + 5165533824X^3 - 8172300544X^2 + 6555431936X - 2157324288,$$

$$P_\infty = 8589934592X^7 + 21474836480X^6 - 867583393792X^5 + 3985729650688X^4 - 6322191859712X^3 + 3298534883328X^2,$$

and finally

$$Q_\infty = -4697620480X^7 + 137438953472X^6 + 1340029796352X^5 - 13726715478016X^4 + 42365557407744X^3 - 62122406969344X^2 + 45079976738816X - 13194139533312.$$

5.2. **Bounding the Faltings height from below.** Let τ lie in the upper half-plane and $q = e^{2\pi i \tau}$. Then

$$\Delta(\tau) = (2\pi)^{12} q \prod_{n \geq 1} (1 - q^n)^{24}$$

defines the discriminant function. It appears in the Faltings height of an elliptic curve E defined over a number field K. Indeed, Suppose that E has complex multiplication. For each embedding $\sigma : K \to \mathbf{C}$ let τ_σ have positive imaginary part and be the quotient of a choice of period lattice basis vectors of the complex elliptic curve induced by E and σ. The stable Faltings height of E is

$$h_F(E) = -\frac{1}{12[K : \mathbf{Q}]} \sum_{\sigma : K \to \mathbf{C}} \log(|\Delta(\tau_\sigma)| \mathrm{Im}(\tau_\sigma)^6) + \frac{1}{2} \log \pi, \tag{28}$$

where $\mathrm{Im}(\cdot)$ denotes the imaginary part of a complex number. Each logarithm in (28) is invariant under the action of $\mathrm{SL}_2(\mathbf{Z})$ by fractional linear transformations on τ_σ. So the local terms are independent of the choice made before. The term $(\log \pi)/2$ is part of Deligne's normalization.

For example, the height of the elliptic curve E with CM by the maximal order in $\mathbf{Q}(\sqrt{-3})$ is

$$h_F(E) = -0.748752485503337827918155520 1 \ldots .$$

Let f be a natural number and p a prime divisor of f. Suppose that χ is a quadratic character and that n is the largest integer with $p^n \mid f$. We set

$$e_f(p) = \frac{1-\chi(p)}{p-\chi(p)} \frac{1-p^{-n}}{1-p^{-1}}. \tag{29}$$

We now make Colmez's Theorem and its extension by Nakkajima-Taguchi explicit. This and an estimate of Badzyan will lead to a lower bound for the height of an elliptic curve with complex multiplication.

Lemma 14. *Let E be an elliptic curve with complex multiplication by an order with discriminant Δf^2 where $f \in \mathbf{N}$ and $\Delta < 0$ is a fundamental discriminant.*

(i) *We have*

$$h_F(E) = \frac{1}{4}\log(|\Delta| f^2) + \frac{1}{2}\frac{L'(\chi,1)}{L(\chi,1)} - \frac{1}{2}\left(\sum_{p\mid f} e_f(p)\log p\right) - \frac{1}{2}(\gamma + \log(2\pi))$$

where the Kronecker symbol $\chi(\cdot) = \left(\frac{\Delta}{\cdot}\right)$ is used in (29) and $\gamma = 0.5772\ldots$ is Euler's constant.

(ii) *We have the estimates*

$$\begin{aligned} h_F(E) &\geq \frac{\sqrt{5}}{20}\log|\Delta| + \frac{1}{2}\log f - 3\log(1+\log f) - \gamma - \frac{\log(2\pi)}{2} \\ &\geq \frac{\sqrt{5}}{20}\log(|\Delta| f^2) - 5.93. \end{aligned}$$

Proof. Part (i) is classical for $f = 1$ and follows from Nakkajima-Taguchi's result [24] in general. For a detailed argument see Lemma 4.1 [11].

To prove the second part we use Badzyan's Theorem 1 [3] which implies

$$\frac{L'(\chi,1)}{L(\chi,1)} + \gamma \geq -\frac{1}{2}\left(1 - \frac{\sqrt{5}}{5}\right)\log|\Delta|.$$

Indeed, the left-hand side is the said author's γ_K with $K = \mathbf{Q}(\sqrt{\Delta})$. Ihara's paper [15] contains bounds subject to the Generalized Riemann Hypothesis.

After rearranging and dividing by 2 we find

$$\frac{1}{4}\log|\Delta| + \frac{1}{2}\frac{L'(\chi,1)}{L(\chi,1)} \geq -\frac{\gamma}{2} + \frac{\sqrt{5}}{20}\log|\Delta|.$$

So

$$h_F(E) \geq \frac{\sqrt{5}}{20}\log|\Delta| + \frac{1}{2}\log f - \frac{1}{2}\left(\sum_{p\mid f} e_f(p)\log p\right) - \gamma - \frac{\log(2\pi)}{2}$$

by part (i).

Below we will show

$$\sum_{p\mid f} e_f(p)\log p \leq 6\log(1+\log f). \tag{30}$$

This inequality implies the first lower bound in (ii) and makes explicit an estimate of Poonen [30].

To prove (30) we may assume $f \geq 2$.

If $\chi(p) = 0$ or 1, then $e_f(p) \leq 1/(p-1)$. Otherwise, $e_f(p) \leq 2/((p+1)(1-1/p)) = 2/(p-1/p)$ from which we deduce $e_f(p) \leq 2/(p-1)$ and $e_f(p) \leq 3/p$. These two inequalities hold regardless of the value of $\chi(p)$.

Let $x > 1$ be a real number, then

$$\sum_{p|f} e_f(p) \log p \leq 3 \sum_{p \leq x} \frac{\log p}{p} + 2 \sum_{p|f, p>x} \frac{\log p}{p-1}.$$

Rosser and Schoenfeld's Corollary to Theorem 6 [31] yields

$$\sum_{p \leq x} \frac{\log p}{p} < \log x.$$

The map $x \mapsto (\log x)/(x-1)$ is decreasing on $(1, \infty)$, so $\sum_{p|f, p>x} \frac{\log p}{p-1} \leq (\log x)\omega(f)/(x-1)$ where $\omega(f)$ denotes the number of distinct prime divisors of f. Combining the bounds for small and large primes yields

$$\sum_{p|f} e_f(p) \log p \leq (\log x) \left(3 + \frac{2\omega(f)}{x-1}\right).$$

A reasonable choice for x is $1 + 2\omega(f)/3 > 1$ which leads to $6 \log(1 + 2\omega(f)/3)$ as an upper bound.

Inequality (30) now follows from the elementary bound $\omega(f) \leq (\log f)/(\log 2)$ which leads to $\log(1 + 2\omega(f)/3) < \log(1 + \log f)$ since $2 < 3 \log 2$.

It remains to show the second inequality in (ii). On taking the derivative we observe that

$$f \mapsto \left(\frac{1}{2} - \frac{\sqrt{5}}{10}\right) \log f - 3 \log(1 + \log f)$$

takes its minimum in $[1, +\infty)$ at $\exp((13 + 3\sqrt{5})/2)$. Thus its minimal value is greater than -4.431 and we conclude

$$\frac{1}{2} \log f - 3 \log(1 + \log f) \geq \frac{\sqrt{5}}{20} \log(f^2) - 4.431.$$

Part (ii) follows since $-4.431 - \gamma - \log(2\pi)/2 \geq -5.93$. □

We define

$$\vartheta(\tau) = 16 e^{\pi i \tau} \prod_{n \geq 1} \left(\frac{1 + e^{2\pi i n \tau}}{1 + e^{2\pi i (n-1/2)\tau}}\right)^8$$

and observe that $\vartheta = 1/(1-\lambda)$ where λ is the the modular function of level 2 as in Section 18.6 [18], cf. Remark 2 in Section 18.4 of loc. cit.

Lemma 15. *If the imaginary part of τ is at least $\sqrt{3}/2$, then*

$$|\Delta(\tau)\vartheta(\tau)^{-2}| \geq 4160174.$$

Proof. The left-hand side of the assertion is

$$2^{-8}(2\pi)^{12} \left| \prod_{n \geq 1} (1 - e^{2\pi i n \tau})^{24} \left(\frac{1 + e^{2\pi i (n-1/2)\tau}}{1 + e^{2\pi i n \tau}}\right)^{16} \right| \geq 2^4 \pi^{12} \prod_{n \geq 1} (1 - q^n)^{24} \left(\frac{1 - q^{n-1/2}}{1 + q^n}\right)^{16}$$

where $q = e^{-\sqrt{3}\pi} \geq |e^{2\pi i\tau}|$. The right-hand side is greater than 4160174. □

Lemma 16. *Let $t \in \overline{\mathbf{Q}} \smallsetminus \{0,1\}$ such that E_t has good reduction everywhere. Then*

$$h_F(E_t) \leq -0.394 + \frac{1}{2}h(t).$$

Proof. The function
(31)

$$\tau \mapsto |\Delta(\tau)|\mathrm{Im}(\tau)^6 \max\left\{|\vartheta(\tau)|, |1-\vartheta(\tau)|, \frac{1}{|\vartheta(\tau)|}, \frac{1}{|1-\vartheta(\tau)|}, \frac{|\vartheta(\tau)|}{|\vartheta(\tau)-1|}, \frac{|1-\vartheta(\tau)|}{|\vartheta(\tau)|}\right\}^2$$

is invariant under the action of $\mathrm{SL}_2(\mathbf{Z})$ on the upper half-plane. If $\sigma : \mathbf{Q}(t) \to \mathbf{C}$ is an embedding, we take τ_σ in the fundamental domain of the $\mathrm{SL}_2(\mathbf{Z})$ action on the upper-half plane and such that $j(\tau_\sigma)$ is the image under σ of the j-invariant of E_t. Thus $\mathrm{Im}(\tau_\sigma) \geq \sqrt{3}/2$ and $\sigma(t)$ equals $\vartheta(\tau_\sigma), 1-\vartheta(\tau_\sigma), 1/\vartheta(\tau_\sigma), 1/(1-\vartheta(\tau_\sigma)), \vartheta(\tau_\sigma)/(\vartheta(\tau_\sigma)-1)$, or $1-1/\vartheta(\tau_\sigma)$. We use Lemma 15 to bound (31) from below by $4160174 \cdot (\sqrt{3}/2)^6 > 1755073$.

We recall (28). Summing over all $\sigma : \mathbf{Q}(t) \to \mathbf{C}$, dividing by $12[K : \mathbf{Q}]$, and adding $\log(\pi)/2$ yields

$$\begin{aligned} h_F(E_t) \leq &-\frac{1}{12}\log(1755073) + \frac{1}{2}\log\pi \\ &+ \frac{1}{6}h([t : 1-t : t^{-1} : (1-t)^{-1} : t(t-1)^{-1} : (1-t)t^{-1}]) \end{aligned}$$

where we use the projective height in the end. After multiplying by $t(t-1)$, the product formula implies that this projective height equals

$$h([t^2(t-1) : t(t-1)^2 : t-1 : t : t^2 : (t-1)^2]).$$

Local considerations at each place show that it is at most $3h(t) + \log 4$. The lemma follows since $-\log(1755073)/12 + \log(\pi)/2 + \log(4)/6 < -0.394$. □

We now complete the proof of Theorem 4. So we assume that E_{-t} has complex multiplication and that $(2,*)$ is a point of finite order n on E_t. We present the discriminant Δf^2 of the endormophism ring of E_{-t} as in Lemma 14. We observe that the inequalities in (ii) hold unchanged as $h(t) = h(-t)$. Together with the previous lemma we obtain $\sqrt{5}\log(|\Delta|f^2)/20 \leq h(t)/2 + 5.536$. We use the height bound (27) to get $|\Delta|f^2 < 2 \cdot 10^{32}$, as desired.

By an estimate involving the analytic class number formula, the number d of positive definite, primitive quadratic forms of discriminant $f^2\Delta$ up-to equivalence satisfies

$$d \leq \frac{6}{2\pi} f|\Delta|^{1/2}(2 + \log(f^2|\Delta|)) \leq 1.1 \cdot 10^{18},$$

cf. Hua's Theorems 12.10.1 and 12.14.3 [13]. Observe that Hua's estimate holds for discriminants that are not necessarily fundamental. This class number is $d = [K(j) : K] = [\mathbf{Q}(j) : \mathbf{Q}]$ where j is the j-invariant of E_{-t}, see Theorem 11.1 [7].

The points $P_t = (2,*), 2P_t, \ldots, (n-1)P_t$ yield at least $(n-1)/2$ distinct abscissas. They all lie in the number field $\mathbf{Q}(t)$ and have height at most $(5h(-t) + \log 58)/3 \leq \log H$

by (26) and (27) from Section 5.1 where $H = 31736$. By Loher's estimate, cf. (1.5) [20], we find

$$\frac{n-1}{2} \leq 37d(\log d)H^{2d} \leq 10^{9.99\cdot 10^{18}}$$

if $d \geq 2$; for $d = 1$ then $\mathbf{Q}(t) \subset \mathbf{Q}(\sqrt{2})$ and left side is bounded by $37 \cdot 2 \cdot (\log 2)H^4$, which is much better. Since $(n-1)/2 \geq n/10$ we find $n \leq 10^{10^{19}}$. □

6. $(2, *)$ is torsion and t is a root of unity $\{3, 4\}$

We consider the pair $\{3, 4\}$. We show the following.

Theorem 5. *There is an absolute effective constant $C > 0$ with the following property. If $t \neq 1$ is a root of unity such that $P = (2, *) \in E_t(\overline{\mathbf{Q}})$ has finite order then the degree of t over $\mathbf{Q}$ is at most C.*

We follow the strategy of [22].

Let

$$\omega_1(t) = \int_1^\infty \frac{dX}{\sqrt{X(X-1)(X-t)}},$$
$$\omega_2(t) = \int_{-i\infty}^0 \frac{dX}{\sqrt{X(X-1)(X-t)}},$$
$$\phi(t) = \frac{1}{2}\int_2^\infty \frac{dX}{\sqrt{X(X-1)(X-t)}}.$$

These are analytic for t with negative real part. Given such a t the values $\omega_1(t), \omega_2(t)$ form a basis for a period lattice of E_t, and $\phi(t)$ is an elliptic logarithm of the point P on E_t. We write $t = x + iy$ with real x and y and let

$$\omega_1(t) = r_1(x, y) + is_1(x, y) \tag{32}$$
$$\omega_2(t) = r_2(x, y) + is_2(x, y) \tag{33}$$
$$\phi(t) = u(x, y) + iv(x, y) \tag{34}$$

where the six functions on the right are real-valued real-analytic functions of x and y. Let

$$\Delta = r_1 s_2 - r_2 s_1. \tag{35}$$

Then for any x, y such that t is in the left half plane $|\Delta(x, y)|$ is the area of any fundamental domain of the lattice determined by $\omega_1(t)$ and $\omega_2(t)$. This area is non-zero, and so the following definitions make sense

$$f_1(x, y) = \frac{u(x, y)s_2(x, y) - v(x, y)r_2(x, y)}{\Delta(x, y)}, \tag{36}$$

$$f_2(x, y) = \frac{-u(x, y)s_1(x, y) + v(x, y)r_1(x, y)}{\Delta(x, y)}. \tag{37}$$

These functions are real-analytic and satisfy

$$\phi(t) = f_1(x, y)\omega_1(t) + f_2(x, y)\omega_2(t). \tag{38}$$

In order to control the roots of unity t such that P is torsion on E_t we shall prove an effective Bombieri-Pila style result for the function $f_1(\cos 2\pi z, \sin 2\pi z)$ for z sufficiently near $1/2$. For this we need to study the continuation of f_1 as a function of two complex variables near the point $(-1,0)$ in $\mathbf{C}^2$.

All the constants asserted to exist below, including implied constants, are absolute and can be effectively computed.

Lemma 17. *There is a $\delta_1 > 0$ and an $M_1 > 0$ such that if $|t+1| \leq \delta_1$ then*

$$\max\{|\omega_1(t)|, |\omega_2(t)|, |\phi(t)|\} \leq M_1.$$

Proof. This follows from Lemma A.2 from [23, Page 477], with $\delta = 1/2$ say, after checking that the absolute constant in Lemma A.1 on the previous page of [23] can be effectively computed. □

Lemma 18. *There is an $\varepsilon > 0$ and an $M_2 > 0$ such that the function $f_1(\cos 2\pi z, \sin 2\pi z)$ has a analytic continuation f to the complex disk $|z - 1/2| \leq \varepsilon$ and on this disk $|f(z)| \leq M_2$.*

Proof. Let $w_1 = x + ix'$ and $w_2 = y + iy'$ be complex variables extending x and y (so x' and y' are real). For $w = (w_1, w_2)$ sufficiently close to $(-1, 0)$ the functions

$$\begin{aligned} \hat{u}(w) &= \frac{1}{2}\left(\phi(w_1 + iw_2) + \overline{\phi(\overline{w_1} + i\overline{w_2})}\right) \\ \hat{v}(w) &= \frac{1}{2}\left(-i\phi(w_1 + iw_2) + \overline{-i\phi(\overline{w_1} + i\overline{w_2})}\right), \end{aligned}$$

where $\bar{\cdot}$ denotes complex conjugation, are analytic, and if $w_1 = x, w_2 = y$ are real then $\hat{u}(w) = u(x,y)$ and $\hat{v}(w) = v(x,y)$. We define complex analytic extensions $\hat{r}_1, \hat{s}_1, \hat{r}_2$ and $\hat{s_2}$ of r_1, s_1, r_2 of s_2 in a similar manner. We use the Euclidean norm on $\mathbf{C}^2$. By Lemma 17, (32), (33) and (34), if $|w - (-1,0)| \leq \delta_1/2$ then

$$\max_{i=1,2}\{|\hat{u}(w)|, |\hat{v}(w)|, |\hat{r}_i(w)|, |\hat{s}_i(w)|\} \leq M_1.$$

We can now define $\hat{\Delta}$ by putting hats on (35), and then if $|w - (-1,0)| \leq \delta_1/2$ we have

$$|\hat{\Delta}(z,w)| \leq 2M_1^2.$$

Using this upper bound for $|\hat{\Delta}|$ we now find a lower bound. First, by Cauchy's inequalities, we have

$$\max\left\{\left|\frac{\partial\hat{\Delta}}{\partial w_1}(w)\right|, \left|\frac{\partial\hat{\Delta}}{\partial w_2}(w)\right|\right\} \leq 4M_1^2\delta_1^{-1} \tag{39}$$

for $|w - (-1,0)| \leq \delta_1/2$. So for such w we have

$$|\hat{\Delta}(w) - \hat{\Delta}(-1,0)| \leq 4\sqrt{2}M_1^2\delta_1^{-1}|w - (-1,0)|. \tag{40}$$

Hence if we take a $\delta_2 < \delta_1/2$ such that $8\sqrt{2}M_1^2\delta_1^{-1}\delta_2 < |\hat{\Delta}(-1,0)|$ then for w with $|w - (-1,0)| \leq \delta_2$ we have

$$|\hat{\Delta}(w)| \geq \frac{|\hat{\Delta}(-1,0)|}{2}. \tag{41}$$

With the lower bound out of the way, we can quickly prove the lemma. First, using the extensions of the real and imaginary parts, we can define a complex-analytic extension $\hat{f}_1$ of f_1 on the set of w in $\mathbf{C}^2$ such that $|w-(-1,0)| \leq \delta_2$. By Lemma 17, the definition of $\hat{f}_1$ and (41) we have

$$|\hat{f}_1(w)| \leq 4M_1^2|\hat{\Delta}(-1,0)|^{-1}.$$

So if we take $\varepsilon > 0$ such that $|(\cos 2\pi z, \sin 2\pi z) - (-1,0)| \leq \delta_2$ for $|z-1/2| \leq \varepsilon$ then the lemma holds, with $M = 4M_1^2|\hat{\Delta}(-1,0)|^{-1}$ (note that $|\hat{\Delta}(-1,0)| = |\Delta(-1,0)|$ is effectively computable, in fact $|\Delta(-1,0)| = \frac{\Gamma\left(\frac{1}{4}\right)^4}{2^3\pi}$). □

To get an effective counting result for the graph of f restricted to a small interval we need some way to count zeros of functions of the form $A(z, f(z))$ for non-zero polynomials A in terms of the degree of A. For this we use a trick from [6], which makes use of the fact that we can also ensure that the coefficients of A are integers and are not too large. The trick relies on f taking a suitable transcendental value at an algebraic number. We will use $f(1/2) = f_1(-1,0)$ and so we now examine this number in more detail. For brevity, we write $a = f_1(-1,0)$. By looking at the integrals defining them, we see that the values $\phi(-1)$ and $\omega_1(-1)$ are both real. So $\omega_2(-1)$ is not real, as $\omega_1(-1)$ and $\omega_2(-1)$ form a basis of a lattice in $\mathbf{C}$. But the functions f_1 and f_2 are real-valued, and so by (38) we find that $f_2(-1,0) = 0$ and so

$$a = \frac{\phi(-1)}{\omega_1(-1)}.$$

Note that E_{-1} has j-invariant 1728 and so by Lemma 6 the point P_{-1} is not torsion on E_{-1}. As $f_2(-1,0) = 0$ is rational, $a = f_1(-1,0)$ is not. Our curve E_{-1} is defined over $\mathbf{Q}$ and so if a were algebraic, then as a ratio of elliptic logarithms it would have to lie in the CM field of E_{-1} and then it would be rational, as it is certainly real. So a is transcendental. In fact it even has a good transcendence measure, as we now observe.

Lemma 19. *There are positive absolute constants μ and ν with the following property. For any integers $T \geq 1$ and $N \geq 3$ and any non-zero polynomial A of degree at most T with integer coefficients of absolute value at most N we have*

$$\log|A(a)| \gg -T^{\mu}(\log N)^{\nu}$$

where the constant implied in Vinogradov's notation is absolute and effective.

Proof. We first find a measure for approximations of a by an algebraic number, α say, of degree T over $\mathbf{Q}$ and height $h(\alpha)$. By Theorem 1.5 on page 42 of [9] (which is far stronger than we need) and with $h = max\{1, h(\alpha)\}$ we have

$$\log|\phi(-1) - \alpha\omega_1(-1)| \gg -T^{\mu'}h^{\nu'},$$

for some positive absolute μ', ν'. So

$$\log|a-\alpha| \gg -T^{\mu'}h^{\nu'}. \tag{42}$$

Now suppose that A is a non-zero polynomial as in the statement, so of degree at most T, and let α be the root of A closest to a. Then

$$|A(a)| \geq |a-\alpha|^{\deg A}. \tag{43}$$

Let B be the minimal polynomial of α over the integers. Then B divides A and so by Lemma 1.6.11 on page 27 of [5] we have

$$|A| \geq 2^{-T}|B|, \tag{44}$$

where $|A|$ and $|B|$ denote the maximum of the absolute values of the coefficients of A and B respectively. By Lemma 3.11 on page 80 of [35], $h(\alpha) \ll 1 + \log|B|$ so by (44) we have

$$h(\alpha) \ll \log N + T,$$

as $|A| \leq N$. Combining this with (43) and (42) gives

$$\log|A(a)| \gg -T^{\mu'+1}\left(\log N + T\right)^{\nu'},$$

which has the required form. □

We can now use the method from [21, 6] to prove an effective bound on the number of rational points of bounded height on the graph of a certain restriction of f. We use the height $H(\alpha) = \exp h(\alpha)$.

Lemma 20. *There are effective absolute constants $\kappa, c > 0$ such that for any integer $H \geq 3$ the number of rationals q of height at most H with $|q - 1/2| \leq \varepsilon/8$ such that $f(q)$ is also a rational of height at most H is at most*

$$c(\log H)^{\kappa}.$$

Proof. Fix an integer $H \geq 3$. In this proof only we write $f_1(z) = z + 1/2$ and $f_2(z) = f(z + 1/2)$. So f_1 is a polynomial, f_2 is analytic on $|z| \leq \varepsilon$ and $|f_1|, |f_2| \leq M$ where $M = \max\{1, M_2\}$, by Lemma 18. Let $\mathcal{Z}$ be the set of rationals q with $|q| \leq \varepsilon/8$ such that $f_1(q), f_2(q)$ are rationals of height at most $2H$. We show that there are at most $c(\log H)^{\kappa}$ points in $\mathcal{Z}$. Put $Z = \varepsilon/2, d = 1$ and $R = 4/\varepsilon$. Then by Proposition 2 on page 2039 of [21] (with A there equal to our R) there is a non-zero polynomial $A(X, Y)$ of degree at most $T \ll \log H$ such that $A(f_1(q), f_2(q)) = 0$ for all q in $\mathcal{Z}$. Examining the proof of Proposition 2 (see the proof of 2.1 in [6]) we find that we can take A to have integer coefficients of absolute value at most $2(T+1)^2(2H)^T$.

If $A(1/2, Y)$ is the zero polynomial then we can divide A by an appropriate power of $(X - 1/2)$ and the resulting polynomial will still vanish at the appropriate points. So we may assume that $P(1/2, Y)$ is not the zero polynomial. By Theorem 1.1 on Page 340 of [19] (see also page 171 in [34]) applied to the disks $|z| \leq \varepsilon/8$ and $|z| \leq \varepsilon/4$ the function $P(f_1(z), f_2(z))$ has at most

$$\frac{1}{\log 2}\left(\log M_A - \log A(\frac{1}{2}, a)\right) \tag{45}$$

zeros in the disk $|z| \leq \varepsilon/8$, where M_A is a bound for the maximum of $A(f_1(z), f_2(z))$ on the disk $|z| \leq \varepsilon/4$. So the cardinality of $\mathcal{Z}$ is also bounded by (45). Using the bounds on $|f_1|$ and $|f_2|$ and on the coefficients of P we find that

$$\log M_A \ll (\log H)^2.$$

And multiplying $A(1/2, a)$ by $2^{\deg A}$ to clear denominators we have a nonzero polynomial in a with integer coefficients to which we can apply Lemma 19. We then find the cardinality of $\mathcal{Z}$ is at most

$$c(\log H)^{\kappa}$$

as required. □

The final ingredients we need are the following bounds on the orders of torsion.

Lemma 21. *Suppose that m and n are positive integers and that t is a root of unity of order m such that P_t has order n on E_t. Then*

$$m \ll [\mathbf{Q}(t) : \mathbf{Q}]^2$$

and

$$n \ll [\mathbf{Q}(t) : \mathbf{Q}]^2.$$

Proof. The second inequality follows from David's Théorème 1.2(i) of [8, Page 106] as in the proof of [22, Lemma 5.1, Page 1685] (since $h(t) = 0$) while the first inequality is classical (for example [12, Theorem 328] is much stronger than we need). □

We can now complete the proof of theorem 5 using the usual argument. So suppose that t is a root of unity of order m such that P_t has order n on E_t, for some positive integers m and n. Let $N = \mathrm{lcm}(m, n)$. Then Lemma 21 gives

$$N \ll d^4 \tag{46}$$

where $d = [\mathbf{Q}(t) : \mathbf{Q}]$. Suppose that t^σ is a Galois conjugate of t. Then t^σ is still a root of unity and $(2, .)$ is still torsion on E_{t^σ}. So t^σ would lead to a rational point of height at most N on the graph of f, if we had $t^\sigma = \exp(2\pi i q)$ for some rational q with $|q - 1/2| \leq \varepsilon/8$. We might not be so lucky, but it is well known that by taking m sufficiently large we can ensure that some fixed positive proportion of the conjugates of t are of this form. So the number, M say, of rational points of height at most N on the graph of f restricted to $|z - 1/2| \leq \varepsilon/8$ satisfies

$$M \gg d.$$

But by Lemma 20 and (46) we have

$$M \ll (\log N)^\kappa \ll (\log d)^\kappa.$$

So d is bounded above by some absolute effective constant. This completes the proof.

References

1. Y. André, *Finitude des couples d'invariants modulaires singuliers sur une courbe algébrique plane non modulaire*, J. Reine Angew. Math. **505** (1998), 203–208.
2. ———, *Shimura varieties, subvarieties, and CM points*, Six lectures at the University of Hsinchu (Taiwan) (with an appendix by C.-L. Chai) `http://math.cts.nthu.edu.tw/Mathematics/lecnotes/andre2001all.ps` (2001).
3. A.I. Badzyan, *The Euler-Kronecker constant*, Mathematical Notes **87** (2010), 31–42.
4. Y. Bilu, D. Masser, and U. Zannier, *An effective "theorem of André" for CM-points on a plane curve*, Math. Proc. Cambridge Philos. Soc. **154** (2013), no. 1, 145–152.
5. E. Bombieri and W. Gubler, *Heights in Diophantine geometry*, New Mathematical Monographs, vol. 4, Cambridge University Press, Cambridge, 2006.
6. G. J. Boxall and G. O. Jones, *Algebraic values of certain analytic functions.*, Int. Math. Res. Not. **2015** (2015), no. 4, 1141–1158 (English).
7. D.A. Cox, *Primes of the form $x^2 + ny^2$*, John Wiley & Sons, 1989.
8. S. David, *Points de petite hauteur sur les courbes elliptiques*, J. Number Theory **64** (1997), no. 1, 104–129.

9. S. David and N. Hirata-Kohno, *Linear forms in elliptic logarithms*, J. Reine Angew. Math. **628** (2009), 37–89.
10. B. Dwork, *p-adic cycles*, Inst. Hautes Études Sci. Publ. Math. (1969), no. 37, 27–115.
11. P. Habegger, *Weakly bounded height on modular curves*, Acta Math. Vietnam. **35** (2010), no. 1, 43–69.
12. G.H. Hardy and E.M. Wright, *An Introduction to the Theory of Numbers*, Oxford University Press, 2005.
13. L. K. Hua, *Introduction to number theory*, Springer-Verlag, Berlin-New York, 1982, Translated from the Chinese by Peter Shiu.
14. D. Husemöller, *Elliptic curves*, second ed., Graduate Texts in Mathematics, vol. 111, Springer-Verlag, New York, 2004, With appendices by Otto Forster, Ruth Lawrence and Stefan Theisen.
15. Y. Ihara, *On the Euler-Kronecker constants of global fields and primes with small norms*, Algebraic geometry and number theory, Progr. Math., vol. 253, Birkhäuser Boston, 2006, pp. 407–451.
16. L. Kühne, *An effective result of André-Oort type*, Ann. of Math. (2) **176** (2012), no. 1, 651–671.
17. ———, *An effective result of André-Oort type II*, Acta Arith. **161** (2013), no. 1, 1–19.
18. S. Lang, *Elliptic Functions*, Springer, 1987.
19. ———, *Complex analysis*, fourth ed., Graduate Texts in Mathematics, vol. 103, Springer-Verlag, New York, 1999.
20. T. Loher and D. Masser, *Uniformly counting points of bounded height*, Acta Arith. **111** (2004), no. 3, 277–297.
21. D. Masser, *Rational values of the Riemann zeta function*, J. Number Theory **131** (2011), no. 11, 2037–2046.
22. D. Masser and U. Zannier, *Torsion anomalous points and families of elliptic curves*, Amer. J. Math. **132** (2010), no. 6, 1677–1691.
23. D. Masser and U. Zannier, *Torsion points on families of squares of elliptic curves*, Math. Ann. **352** (2012), no. 2, 453–484.
24. Y. Nakkajima and Y. Taguchi, *A generalization of the Chowla-Selberg formula*, J. Reine Angew. Math. **419** (1991), 119–124.
25. J.L. Parish, *Rational torsion in complex-multiplication elliptic curves*, J. Number Theory **33** (1989), no. 2, 257–265.
26. R. Paulin, *An explicit André-Oort type result for* $\mathbb{P}^1(\mathbb{C}) \times \mathbb{G}_m(\mathbb{C})$ *based on logarithmic forms*, Preprint 2014.
27. ———, *An explicit André-Oort type result for* $\mathbb{P}^1(\mathbb{C}) \times \mathbb{G}_m(\mathbb{C})$, Math. Proc. Cambridge Philos. Soc. **159** (2015), no. 1, 153–163.
28. J. Pila, *Rational points of definable sets and results of André-Oort-Manin-Mumford type*, Int. Math. Res. Not. IMRN (2009), no. 13, 2476–2507.
29. ———, *O-minimality and the André-Oort conjecture for* $\mathbb{C}^n$, Ann. of Math. (2011), no. 173, 1779–1840.
30. B. Poonen, *Spans of Hecke Points on Modular Curves*, Mathematical Research Letters **8** (2001), 767–770.
31. J.B. Rosser and L. Schoenfeld, *Approximate formulas for some functions of prime numbers*, Illinois J. Math. **6** (1962), 64–94.
32. J.H. Silverman, *The Arithmetic of Elliptic Curves*, Springer, 1986.
33. M. Stoll, *Simultaneous torsion in the Legendre family*, Preprint,arXiv:1410.7070 (19 pages).
34. E.C. Titchmarsh, *The theory of functions*, Oxford University Press, 1939.
35. M. Waldschmidt, *Diophantine approximation on linear algebraic groups*, Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences], vol. 326, Springer-Verlag, Berlin, 2000, Transcendence properties of the exponential function in several variables.
36. P. J. Weinberger, *Exponents of the class groups of complex quadratic fields*, Acta Arith. **22** (1973), 117–124.
37. G. Wüstholz, *A note on the conjectures of André-Oort and Pink with an appendix by Lars Kühne*, Bull. Inst. Math. Acad. Sin. (N.S.) **9** (2014), no. 4, 735–779, With an appendix by Lars Kühne.

(P. Habegger) University of Basel, Spiegelgasse 1, 4051 Basel, Switzerland
E-mail address: philipp.habegger@unibas.ch

(G. Jones) School of Mathematics, University of Manchester, Oxford Road, Manchester, M13 9PL, UK
E-mail address: gareth.jones-3@manchester.ac.uk

(D. Masser) University of Basel, Spiegelgasse 1, 4051 Basel, Switzerland
E-mail address: david.masser@unibas.ch

LATEST PREPRINTS

No.	Author: *Title*
2015-06	**S. Iula, A. Maalaoui, L. Martinazzi** *A fractional Moser-Trudinger type inequality in one dimension and its critical points*
2015-07	**A. Hyder** *Structure of conformal metrics on R^n with constant Q-curvature*
2015-08	**M. Colombo, G. Crippa, S. Spirito** *Logarithmic Estimates for Continuity Equations*
2015-09	**M. Colombo, G. Crippa, S. Spirito** *Renormalized Solutions to the Continuity Equation with an Integrable Damping Term*
2015-10	**G. Crippa, N. Gusev, S. Spirito, E. Wiedemann** *Failure of the Chain Rule for the Divergence of Bounded Vector Fields*
2015-11	**G. Crippa, N. Gusev, S. Spirito, E. Wiedemann** *Non-Uniqueness and Prescribed Energy for the Continuity Equation*
2015-12	**G. Crippa, S. Spirito** *Renormalized Solutions of the 2D Euler Equations*
2015-13	**G. Crippa, E. Semenova, S. Spirito** *Strong Continuity for the 2D Euler Equations*
2015-14	**J. Diaz, M. J. Grote** *Multi-Level Explicit Local Time-Stepping Methods for Second-Order Wave Equations*
2015-15	**F. Da Lio, L. Martinazzi, T. Riviere** *Blow-up analysis of a nonlocal Liouville-type equation*
2015-16	**A. Maalaoui, L. Martinazzi, A. Schikorra** *Blow-up behaviour of a fractional Adams-Moser-Trudinger type inequality in odd dimension*
2015-17	**T. Boulenger, E. Lenzmann** *Blowup for Biharmonic NLS*
2015-18	**D. Masser, U. Zannier (with Appendix by V. Flynn)** *Torsion point on families of simple abelian surfaces and Pell's equation over polynomial rings*

Preprints are available under *https://math.unibas.ch/research/publications*

LATEST PREPRINTS

No.	Author: *Title*
2015-19	**M. Bugeanu, R. Di Remigio, K. Mozgawa, S. S. Reine, H. Harbrecht, L. Frediani** *Wavelet Formulation of the Polarizable Continuum Model. II. Use of Piecewise Bilinear Boundary Elements*
2015-20	**J. Dölz, H. Harbrecht, M. Peters** *An interpolation-based fast multipole method for higher order boundary elements on parametric surfaces*
2015-21	**A. Schikorra** *Nonlinear Comutators for the fractional p-Laplacian and applications*
2015-22	**L. Martinazzi** *Fractional Adams-Moser-Trudinger type inequalities*
2015-23	**P. Habegger, J. Pila** *O-Minimality and certain atypical intersections*
2015-24	**P. Habegger** *Singular Moduli that are Algebraic Units*
2015-25	**P. Habegger, F. Pazuki** *Bad Reduction of genus 2 curves with CM jacobian varieties*
2015-26	**A. Bohun, F. Bouchut, G. Crippa** *Lagrangian solutions to the 2D Euler system with L^1 vorticity and infinite energy*
2015-27	**A.-L. Haji-Ali, H. Harbrecht, M. Peters, M. Siebenmorgen** *Novel results for the anisotropic sparse quadrature and their impact on random diffusion problems*
2015-28	**P. Habegger, G. Jones, D. Masser** *Six unlikely intersection problems in search of effectivity*

Preprints are available under *https://math.unibas.ch/research/publications*