Counting rational points on elliptic curves with a rational 2-torsion point

Francesco Naccarato

June 2020

ABSTRACT. Let $E/\mathbb{Q}$ be an elliptic curve over the rational numbers. It is known, by the work of Bombieri and Zannier, that if E has full rational 2-torsion, the number $N_E(B)$ of rational points with Weil height bounded by B is $O_\epsilon(B^\epsilon)$ for every positive ϵ, and more precisely $B^{O\left(\frac{1}{\sqrt{\log\log B}}\right)}$. In this paper we exploit the method of descent via 2-isogeny to extend this result to elliptic curves with at least one nontrivial rational 2-torsion point. Moreover, we make use of a result of Petsche to derive the stronger upper bound $N_E(B) = B^{O\left(\frac{1}{\log\log B}\right)}$ for these curves and to remove a deep transcendence theory ingredient from the proof.

1 Introduction and results

For an elliptic curve $E/\mathbb{Q}$ in Weierstrass form given by an affine equation:

$$y^2 = x^3 + ax^2 + bx + c \qquad a, b, c \in \mathbb{Q} \tag{1}$$

we define its (naive) height $H(E)$ as the Weil height of the vector $(1, a, b, c)$, its discriminant Δ_E as 16 times the discriminant of the polynomial on the right-hand side (which is nonzero by the nonsingularity of elliptic curves) and we let $h(E) := \log H(E)$.
Recall that a Weierstrass equation for E is called a *minimal model* at a prime p if the p-adic valuation of the relative discriminant is the smallest possible (that is, an integer $0 \leq m < 12$). An equation which is a minimal model at all primes is called a (global) minimal model.
We will see that it is not restrictive to work with a quasi-minimal model (one that is minimal at all primes p except at most 2 and 3) of E, given by:

$$y^2 = x^3 + Ax + B \tag{2}$$

with $A, B \in \mathbb{Z}$. We see that in this case $\Delta_E = -16(4A^3 + 27B^2)$, so we have:

$$|\Delta_E| \leq 496 H(E)^3. \tag{3}$$

We recall that the points of an elliptic curve defined over $\mathbb{C}$ form a group with the usual structure arising from the Weierstrass map. When E is defined over $\mathbb{Q}$, the set of its rational points is a finitely generated subgroup, the Mordell-Weil group $E(\mathbb{Q})$; the rank r_E is defined as the abelian rank of $E(\mathbb{Q}) \simeq \mathbb{Z}^{r_E} \times T$, where T is the torsion subgroup.
Let us introduce the usual Weil height $H(P)$ of a rational point as the Weil height of its x-coordinate, and its logarithmic analogue as $h(P) := \log H(P)$.
Moreover, let us define the quantity that we are interested in bounding:

$$N_E(B) := |\{P \in E(\mathbb{Q}) : H(P) \leq B\}|$$

or, equivalently,

$$N_E(B) := |\{P \in E(\mathbb{Q}) : h(P) \leq \log B\}|. \tag{4}$$

We will from now on omit the subscript E on Δ, r and $N(B)$, keeping in mind the dependence of these quantities on the curve.
In [1], Theorem 1, Bombieri and Zannier proved that for elliptic curves in Weierstrass form with full rational 2-torsion one has:

$$N(B) \leq B^{\frac{c}{\sqrt{\log\log B}}}$$

for sufficiently large B (depending on the curve), with c an absolute constant.

We can now state our result:

Theorem 1.1. *There exists an absolute computable constant C such that for any elliptic curve $E/\mathbb{Q}$ as in* (1) *with a rational* 2*-torsion point the inequality:*

$$N(B) \leq M^{\frac{C}{\log\log M}} \tag{5}$$

holds, with $M := \max\{B, H(E), e^3\}$.

This result implies, for this special family of curves, a conjecture that is widely believed to hold true for any elliptic curve over $\mathbb{Q}$ in Weierstrass form:

Conjecture 1. *Let $\epsilon > 0$. There exists a constant $c'(\epsilon)$ depending only on ϵ such that, with the same notation as in Theorem 1.1,*

$$N(B) \leq c'(\epsilon) M^{\epsilon}$$

for any elliptic curve $E/\mathbb{Q}$ as in (1).

We are able to obtain our improved upper bound for $N(B)$ by making use of a result of Petsche [2], which we will state in Section 3, giving a lower bound for the smallest height of a non-torsion point that depends polynomially on the *Szpiro ratio* of the curve. By contrast, the lower bound for the same quantity used in [1] depends exponentially on the *Szpiro ratio* (see Theorem 0.3 in Hindry and Silverman's work [3]), and turns out to be useful only if the rank of the curve is large enough. For small ranks, Bombieri and Zannier employed a

result of Masser (see [4], Theorem), whose proof relies on transcendence theory techniques. Hence, by removing the need for this result, we are considerably simplifying the proof structure.
Furthermore, as we will see in Section 4, even assuming Lang's height conjecture for rational elliptic curves, which improves on Petsche's estimate for the smallest canonical height by removing the dependence on the *Szpiro ratio*, does not lead to an improvement on our result.

The need for a single 2-torsion point comes from the fact that it turns out to be sufficient to effectively bound the rank of the curve in terms of the discriminant, as we will illustrate in the next section.
In what follows, the numbers c_k will be positive, absolute and computable constants.

For our estimation, we make use of the canonical height:

$$\hat{h}(P) := \lim_{n\to\infty} 4^{-n} h(2^n P).$$

It is well known that $\hat{h}$ is a quadratic form on $E(\mathbb{Q})$ and that it is positive definite on the quotient $E(\mathbb{Q})/T \simeq \mathbb{Z}^r$. If we consider the tensor product of abelian groups $E(\mathbb{Q}) \otimes \mathbb{R} \simeq \mathbb{R}^r$, we see that the torsion is mapped in 0 by the tensor, and $E(\mathbb{Q})/T$ injects (in the sense of $E(\mathbb{Q})/T \otimes 1 \hookrightarrow E(\mathbb{Q}) \otimes \mathbb{R}$) in a lattice $\mathcal{L}_E$ of dimension r: we can then bring our quadratic form onto this lattice by setting $\hat{h}(x) := \hat{h}(P)$ where P is the unique rational point modulo torsion such that $P \otimes 1 = x$.
This form can be extended by linearity to $\mathbb{Q}^r$ and by continuity to all $\mathbb{R}^r$, and it is a well-known result that it remains positive definite: hence, we can take $\hat{h}$ to be the square of the usual euclidean norm (so $\mathcal{L}_E$ won't necessarily be $\mathbb{Z}^r$ in a metric sense).

Zimmer [5] proved that, for a fixed curve in Weierstrass model
$Y^2 = 4X^3 - g_2 X - g_3$, the Weil and canonical heights differ by at most a constant. As remarked in [1], this is easily extended to models as in (1), so proving (5) for the Weil height with $N(B)$ defined as in (4) is equivalent to proving it with the alternative definition:

$$N(B) := |\{P \in E(\mathbb{Q}) : \hat{h}(P) \leq \log B\}|.$$

The problem of counting rational points with Weil height up to B is thus equivalent to that of counting the number of points of $\mathcal{L}_E$ in the ball of centre 0 and radius $\sqrt{\log B}$, and then multiplying by the cardinality of the torsion. We immediately remark that for elliptic curves over $\mathbb{Q}$ the cardinality of the torsion is known to be absolutely bounded by the work of Mazur [6].

Remark 1.2. To see that it is sufficient to prove Theorem 1.1 for curves as in (2), just notice that given a model E' as in (1), the usual translation-dilation isomorphism $\phi : E' \to E$ to the respective model as in (2) preserves the canonical height, and that $h(E') \leq c_0 h(E) + c_0$.

2 Bounding the rank

As we will see in the next section, in order for our methods to work on a given elliptic curve it is crucial to have an upper bound on its rank. If our curve has a rational 2-torsion point, a good upper bound in terms of the discriminant can be obtained in a simple way through a descent via 2-isogeny.

Lemma 2.1. *Let $E/\mathbb{Q}$ be an elliptic curve as in (2) with a rational 2-torsion point. Let Δ be its discriminant and r its rank: then one has*

$$r \leq 2w(\Delta) + 2. \tag{6}$$

where $w(m)$ is the number of distinct prime factors of the integer m.

Proof: We can apply a descent via 2-isogeny as described in [7] (see specifically p.92, Proposition 3.8 and p.98), obtaining:

$$|E(\mathbb{Q})/2E(\mathbb{Q})| \leq 2^{w(\Delta)+2}.$$

This, together with the bound

$$2^r \leq |E(\mathbb{Q})/2E(\mathbb{Q})|,$$

which follows by explicitly writing the quotient as

$$(\mathbb{Z}/2\mathbb{Z})^r \prod_{i=1}^{k} \mathbb{Z}_{p_i^{r_i}}/2\mathbb{Z}_{p_i^{r_i}}$$

thanks to the classification of finitely generated abelian groups, gives:

$$r \leq 2w(\Delta) + 2. \quad \square$$

We now observe that the *Prime Number Theorem* implies the bound:

$$w(m) = O\left(\frac{\log m}{\log\log m}\right).$$

This, together with (6), tells us that for curves as in (2) we have:

$$r \leq c_1 \frac{\log|\Delta|}{\log\log|\Delta|}$$

This estimation is the key point where the rationality of a 2-torsion point comes into play: in fact, in all that follows we can drop this assumption.

Remark 2.2. Notice that in proving Theorem 1.1 we can suppose, without loss of generality,

$$B \geq \max\{H(E), e^3\}.$$

This is because if $B < \max\{H(E), e^3\}$ then $N(B) \leq N(\max\{H(E), e^3\})$ and they have the same upper bound in the statement. We need $B \geq e^3$ simply to ensure that $\log\log B > 1$ in what follows.

Remark 2.2, along with (3), tells us that we can work with $\log B \geq c_2 \log |\Delta|$, from which we obtain:

$$r \leq c_3 \frac{\log B}{\log \log B}. \tag{7}$$

3 Counting through a covering argument in $\mathbb{R}^n$

We will apply the following well-known counting strategy:

1. we find a small enough radius ρ_0 such that we can ensure that any ball of radius ρ_0 centered at a point of $\mathcal{L}_E$ does not contain any other point of $\mathcal{L}_E$;
2. we count how many of these balls we need to cover the intersection of $\mathcal{L}_E$ with the ball of centre 0 and radius $\sqrt{\log B}$.

This is almost the same strategy followed by Bombieri and Zannier in [1]: the only substantial difference is that they work with two different values of ρ_0 depending on the magnitude of the rank, and for one of these values the number of lattice points inside the small balls is not necessarily 1, but some computable constant.
For the reader's convenience, we repeat the lemmas and proofs that can already be found in [1].

The second step of the strategy is the easiest, for we just need an elementary covering lemma:

Lemma 3.1. *Given a positive integer n, radii R, ρ and a subset S of the n-ball $\mathcal{B}_n(0,R)$, there exists a set of at most $(1+\frac{2R}{\rho})^n$ balls of radius ρ centered at points of S such that S is contained in the union of these balls.*

Proof: Consider a maximal set Γ of disjoint balls of radii $\frac{\rho}{2}$ centered at points of S (by maximal we mean such that any ball of radius $\frac{\rho}{2}$ centered at a point of S intersects a ball of Γ). Notice that the union of the balls in Γ is contained in $\mathcal{B}_n(0, R+\frac{\rho}{2})$, which gives

$$|\Gamma| \leq \frac{V_n(R+\frac{\rho}{2})}{V_n(\frac{\rho}{2})} \leq \left(1+\frac{2R}{\rho}\right)^n$$

with $V_n(a)$ the n-volume of the n-ball of radius a.
But enlarging the balls in Γ by a factor of 2 we get a set of balls centered at points of S which covers S, because if a point of S lied outside the union of these new balls, that would contradict maximality. $\square$

It is clear that we will make use of this lemma putting $n = r$ (and $R = \sqrt{\log B}$, $\rho = \rho_0$), from which the importance of the magnitude of the rank in our estimation follows.

A good value for ρ_0 is derived by Petsche in [2]. It turns out that the minimum canonical height of a non-torsion point can be bounded below as a function of the minimal discriminant $\mathcal{D}$ of E (that is, the discriminant of one of its minimal models) and of its *Szpiro ratio*:

$$\sigma = \frac{\log |\mathcal{D}|}{\log \mathcal{N}}$$

where $\mathcal{N}$ is the conductor of the curve.

Remark 3.2. If $\mathcal{N} = 1$ then it is known that $\mathcal{D} = 1$ and σ is defined to be 1.

Remark 3.3. Recall that the prime factors of the minimal discriminant of an elliptic curve $E/\mathbb{Q}$ are exactly the primes of bad reduction for E, while the discriminant Δ of our quasi-minimal model has an additional factor $2^j 3^k$ with $j, k \in \mathbb{N}$. For the definition of the conductor and the proof that $\sigma \geq 1$ see, for example, [2].

Proposition 3.4 (Petsche, [2])**.** *There exist constants $c_4, c_5 > 1$ such that for any non-torsion point $P \in E(\mathbb{Q})$, we have:*

$$\hat{h}(P) \geq \frac{\log |\mathcal{D}|}{c_4 \sigma^6 \log^2(c_5 \sigma)}.$$

Notice that $\log^2(c_5\sigma) < c_5^2\sigma^2$, so we have:

$$\hat{h}(P) > \frac{\log |\mathcal{D}|}{c_6 \sigma^8}. \tag{8}$$

Observe that since no elliptic curve over $\mathbb{Q}$ has everywhere good reduction, $|\mathcal{D}| > 1$ and our lower bound is positive. For the same reason, Remark 3.2 implies that $\mathcal{N} \geq 2$. Let us now apply Lemma 3.1 with $\rho = \sqrt{\frac{\log |\mathcal{D}|}{c_6 \sigma^8}}$; then we know that in each of the balls of this radius centered at points of $\mathcal{L}_E$ there is just one non-torsion point (that is, the centre) and so we obtain:

$$N(B) \leq |T| \left(1 + 2c_6 \sqrt{\frac{\log B}{\log |\mathcal{D}|}} \sigma^4\right)^r \leq c_7 \left(c_8 \frac{\log B}{log \mathcal{N}} \sigma^3\right)^r \tag{9}$$

since surely $|\mathcal{D}| \leq |\Delta|$.
Observe that for the set of curves of rank bounded by any fixed absolute constant c_9 the statement of Theorem 1.1 clearly follows from (9), since in this case we can just directly bound $\log \mathcal{N} \geq \log 2$, $\sigma \leq 2 \log |\mathcal{D}| \leq 2c_2 \log B$ and get:

$$N(B) \leq c_7 (c_{10} \log B)^{4c_9} \leq (\log B)^{c_{11}} \leq B^{\frac{c_{11}}{\log \log B}}.$$

So from now on we can consider, for example, $r \geq 39$. Notice that this in turn requires B to be not too small.
Since, by [8], Appendix C, Table 15.1, $\mathcal{N}$ is divisible by all the primes dividing

$\mathcal{D}$ except at most 2 and 3, and hence by all the primes dividing Δ except at most 2 and 3, it follows from Lemma 2.1 that $6\mathcal{N}$ has at least $\max\{2, \frac{r-2}{2}\} \geq \frac{r}{3}$ prime factors and hence we have:

$$6\mathcal{N} \geq p_{\frac{r}{3}}\# \tag{10}$$

with $p_n\# := \prod_{j=1}^{n} p_j$ the product of the first n primes.

Lemma 3.5. *For $n \geq 13$ the inequality:*

$$p_n\# \geq n^n$$

holds.

Proof: This is easily verified with a calculator for $n = 13$, and then we can proceed by induction: for the inductive step we just need $p_n \geq \frac{n^n}{(n-1)^{n-1}}$. But $\frac{n^n}{(n-1)^{n-1}} \leq n\left(1 + \frac{1}{n-1}\right)^{n-1} \leq en$ and $p_n > nlogn > en$ by Rosser's theorem [9] and the fact that $p_n \geq 43 > e^e$. $\square$

Lemma 3.5 and (10) give us:

$$\log 6 + \log \mathcal{N} \geq \frac{r}{3} \log \frac{r}{3}.$$

For $r \geq 39$ we obtain $\log \mathcal{N} \geq \frac{r \log r}{7}$ and consequently $\sigma \leq \frac{7c_2 \log B}{r \log r}$. Substituting in (9) we are left with the task of showing that the maximum of the function

$$f(x) = c_7 \left(c_{12} \frac{\log B}{x \log x} \right)^{c_{13} x}$$

for $x \in [39,\ c_3 \frac{\log B}{\log \log B}]$ is $B^{O(\frac{1}{\log \log B})}$.

This is done as follows: clearly we can forget about the constants c_7 and c_{13}. We can also forget about c_{12} precisely because $x = O\left(\frac{\log B}{\log \log B}\right)$. Write:
$A = \log B$, $f(x) = \exp(x(\log A - \log(x \log x)))$.
The derivative

$$f'(x) = f(x)[\log A - (\log(x \log x) + 1 + \frac{1}{\log x})] =: f(x)g(x)$$

is positive for x up to a certain value x_0 that satisfies $x_0 \log x_0 \sim \frac{A}{e}$ and negative afterwards (since $x \geq 39$ we don't have to worry about the term $\frac{1}{\log x}$ being big). Formally, for $x \geq 39$, $g(x)$ is a decreasing function in x, which is nonnegative for $x \log x = Ae^{-1-\frac{1}{\log 39}}$ and negative for $x \log x = A$.
This in particular tells us that the zero x_0 of $f'(x)$ satisfies $x_0 \leq 2\frac{A}{\log A}$ and hence:

$$f(x) \leq \exp\left(2\left(1 + \frac{1}{\log 39}\right)\frac{A}{\log A}\right) = B^{O(\frac{1}{\log \log B})}$$

as required.

4 Some remarks and further explorations

It is interesting to observe that, even if we had a lower bound

$$\hat{h}(P) \gg \log |\mathcal{D}|,$$

independent of σ, which is Lang's height conjecture for elliptic curves over $\mathbb{Q}$ (or even just for those with a rational 2-torsion point), we could not improve on Theorem 1.1 by means of our methods: in fact, we would have to bound

$$\left(\frac{\log B}{\log |\mathcal{D}|}\right)^r$$

for $\log |\mathcal{D}|$ and r in the ranges given by (3) and (7). Choosing $\log B = c_{14} \log |\mathcal{D}|$ and clearly r as big as possible, we get exactly the result we already proved:

$$N(B) \leq e^{c_{15} \frac{\log B}{\log \log B}} = B^{\frac{c_{15}}{\log \log B}}.$$

This hints that, in order to improve on our bound for $N(B)$, one should improve on the estimate for the rank in terms of the discriminant (at least for our special class of curves; moreover, obtaining any sensible estimate of this kind for a broader class of curves could help in establishing Conjecture 1 for more elliptic curves). As an extreme example, observe that uniform boundedness of the ranks would give an upper bound of $(\log B)^{O(1)}$ for $N(B)$.

We point out that our upper bound for $N(B)$ is barely insufficient for what would have been an interesting application: in [10] Bombieri and Bourgain study a certain property of the solutions to the diophantine equation $x^2 + y^2 = m$. Specifically, they are interested in finding an asymptotic upper bound to the cardinality of the set

$$S_6(m) = \{(\lambda_1, ..., \lambda_6) \in \Lambda_m^6 : \lambda_1 + \lambda_2 + \lambda_3 = \lambda_4 + \lambda_5 + \lambda_6\}$$

where Λ_m is the set of the gaussian integers λ such that $\lambda\bar{\lambda} = m$. Setting $N = |\Lambda_m|$ the number of solution to the equation of interest, their goal is to prove that one has: $|S_6(m)| = O(N^{3+\epsilon})\ \forall \epsilon > 0$.
Tackling this problem through the theory of elliptic curves, and specifically by reducing it to the task of counting rational points on certain families of elliptic curves associated to the parameter m, they are able to prove a weak conditional result (Theorem 8), that we restate here for the reader's convenience:

Theorem 4.1 (Bombieri, Bourgain)**.** *At least one of the two following statements holds.*

1. *If* $\frac{\log N}{\log \log m} \to \infty$*, then* $|S_6(m)| = O(N^{3+o(1)})$.
2. *There exist elliptic curves* $E/\mathbb{Q}$ *of unbounded rank.*

It would be interesting to remove the condition on the ranks, which appears to be far from easy to settle. Since the curves they deal with have a rational 2-torsion point, we can apply our result to their methods and remove the dependence from the rank. By doing this, one sees that the first condition has to be weakened to $\frac{\log N \log\log m}{\log m} \to \infty$, which turns out to be vacuous because $\log N = O\left(\frac{\log m}{\log\log m}\right)$, as can be inferred by writing explicitly N as in [10], (20).
Any asymptotic improvement on our bound would instead imply the conjecture for the family:

$$\{m : \log N \geq A\frac{\log m}{\log\log m}\}$$

for any fixed $A > 0$, which for sufficiently small A is nonempty (it contains the products of the first k primes congruent to 1 mod 4, for example).
We remark that in [10] Bombieri and Bourgain prove a probabilistic analogue of this (conjectural) result for squarefree m, conditional on the Birch and Swinnerton-Dyer conjecture and on a Riemann Hypothesis.

Even though it does not lead to any quantitative improvement in our estimate, other than the change of an absolute constant, it is interesting to notice that Petsche's lower bound for the smallest canonical height, which in the original paper is established for curves over arbitrary number fields and depends also on the degree of the number field, can be slightly improved for curves over $\mathbb{Q}$. In particular, we can remove the $\log^2(c_5\sigma)$ factor from the statement of Proposition 3.4; we recall for the reader's convenience Proposition 8 of [2]:

Let k a number field of degree $d = [k : \mathbb{Q}]$, and let E/k be an elliptic curve with Szpiro ratio σ. Then:

$$|\{P \in E(k) : \hat{h}(P) \leq \frac{\log \mathbb{N}_{k/\mathbb{Q}}(\Delta_{E/k})}{2^{13}3d\sigma^2}\} \leq a_1 d\sigma^2 \log(a_2 d\sigma^2)$$

with $a_1 = 134861$ and $a_2 = 104613$.

In its proof in the original paper, we see that in the precise case of $k = \mathbb{Q}$ that we are examining, the left-hand side of (25) is precisely 0 since $\mathbb{Q}$ has just one archimedean place, and no estimate is needed. This enables us to remove the $\log(a_2 d\sigma^2)$ factor in the statement of Proposition 8. The rest of the proof remains unchanged.
As remarked by Petsche, this also holds for imaginary quadratic fields, since they, too, have just one archimedean place.

Acknowledgments

The author would like to thank Professor Umberto Zannier for the invaluable guidance and suggestions, not only of a mathematical nature, which he offered throughout the process of writing this paper.
The author would also like to thank Professor Clayton Petsche for the helpful discussion concerning his work.

References

[1] E. Bombieri and U. Zannier. On the number of rational points on certain elliptic curves. *Izvestiya Mathematics 68*, 2004.

[2] C. Petsche. Small rational points on elliptic curves over number fields. *The New York Journal of Mathematics [electronic only] Volume: 12, page 257-268*, 2006.

[3] M. Hindry and J. H. Silverman. The canonical height and integral points on elliptic curves. *Inventiones Mathematicae, 93: 419–450*, 1988.

[4] D.W. Masser. Counting points of small height on elliptic curves. *Bulletin de la S. M. F., tome 117, no 2 (1989), p. 247-265*, 1989.

[5] H.G. Zimmer. On the difference of the Weil height and the Néron-Tate height. *Math. Z. 147, 35-51*, 1976.

[6] B. Mazur. Rational isogenies of prime degree. *Inventiones Mathematicae, 44 (2): 129–162*, 1978.

[7] J. H. Silverman and J. T. Tate. *Rational Points on Elliptic Curves*. Springer, 2015.

[8] J. H. Silverman. *The Arithmetic of Elliptic Curves*. Springer-Verlag, 2009.

[9] B. Rosser. The n-th prime is grater than $n \log n$. *Proceedings of the London Mathematical Society*, 1939.

[10] E. Bombieri and J. Bourgain. A problem on sums of two squares. *International Mathematics Research Notices, Vol. 2015, No. 11, pp. 3343–3407*, 2015.