Counting rational points on elliptic curves and descent via 2-isogeny

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, then the number $N_E(B)$ of rational points with Weil height bounded by B is $\mathcal{O}_\epsilon(B^\epsilon)$ for every positive ϵ. In this work, we exploit the method of descent via 2-isogeny to extend this result to the case in which E has just one rational 2-torsion point. Moreover, we make use of a result of Petsche to improve on the best known estimate for the growth of $N_E(B)$ for this class of curves.

1 Notation

We denote the cardinality of a set X as $|X|$.

The numbers c_k in the following will be positive, absolute and computable constants.

We will write $f(x) << g(x)$ to mean that $\exists \lim_{x\to\infty} \frac{f(x)}{g(x)} < \infty$.

The function $w(\cdot)$ counts the number of distinct prime factors of the integer input.

We will initially define quantities that depend on an elliptic curve E by putting E in subscript, but will subsequently omit this.

2 Introduction and results

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

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

we define, in the usual fashion, its height $H(E)$ as the Weil height of the vector $(1, a, b)$, its discriminant $\Delta_E := -16(4a^3 + 27b^2)$ and we let $h(E) := \log H(E)$.

We will see that it is not restrictive to work with a quasi-minimal model of E, given by:

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

with $A, B \in \mathbb{Z}$ and $H(E) = max\{4|A|^3, 27B^2\}$.
We recall that elliptic curves are groups with the usual structure arising from the Weierstrass map. When E is an elliptic curve defined over $\mathbb{Q}$, the set of its rational points is a subgroup, the Mordell-Weil group $E(\mathbb{Q})$. We also recall that, by Mordell's Theorem, $E(\mathbb{Q})$ is finitely generated and that the rank r_E is defined as the abelian rank of $E(\mathbb{Q}) \equiv \mathbb{Z}^{r_E} \times T$.
We will say that an elliptic curve $E/\mathbb{Q}$ has a rational 2-torsion point when the 2-torsion subgroup of E, denotad as $E[2]$, intersects its Mordell-Weil group non-trivially; we will say that E has full rational 2-torsion when $E[2] \subset E(\mathbb{Q})$.
Let us introduce the usual Weil height $H(P)$ of a rational point as the Weil height of its x-coordinate, and analogously for its logarithmic Weil height. 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,

$$N_E(B) := |\{P \in E(\mathbb{Q}) : h(P) \leq \log B\}| \tag{3}$$

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) and C an absolute constant.

We can now state our result:

Theorem 2.1 *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:*

$$N(B) \leq M^{\frac{c}{\log \log M}} \tag{4}$$

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

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

Conjecture 1 *Let $\epsilon > 0$. There exists a constant $c'(\epsilon)$ depending only on ϵ such that, with the same notation as in Theorem 2.1,*

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

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

3 Preliminaries

We start by noticing that

$$|\Delta| \leq 32H(E). \tag{5}$$

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 $E(\mathbb{Q})/T \simeq \mathbb{Z}^r$. We can 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 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 the image lattice of the Mordell-Weil group modulo torsion will be some lattice, not necessarily $\mathbb{Z}^r$, in a metric sense).
It is well known (see [2]) that, once the curve is fixed, the Weil and canonical heights differ by at most a constant, so proving (4) for the Weil height with $N(B)$ defined as in (3) is equivalent to proving it with the alternative definition

$$N(B) := |\{P \in E(\mathbb{Q}) : \hat{h}(P) \leq \log B\}|. \tag{6}$$

Hence the problem of counting rational points with Weil height up to $\log B$ is the same as counting the number of the points of this lattice in the ball of centre 0 and radius $\sqrt{\log B}$, and then multiplying by the cardinality of the torsion.

Remark 3.1 *To see that it is sufficient to prove Theorem 2.1 for curves as in (2), just notice that changing from a model E' as in (1) to one E as in (2) does not change the canonical height, and that $h(E') \leq c_0 h(E) + c_0$.*

Lemma 3.2 *Let $E/\mathbb{Q}$ be an elliptic curve in Weierstrass form with a rational 2-torsion point. Let Δ be its discriminant and r its rank: then one has*

$$r \leq 2w(\Delta) + 2. \tag{7}$$

Proof: We can apply a descent via 2-isogeny as described in [3] (see specifically Prop. 3.8 p.92 and p. 98) to obtain:

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

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:

$$w(k) << \frac{\log k}{\log \log k}$$

This, together with (7), tells us that $r \leq c_1 \frac{\log |\Delta|}{\log \log |\Delta|} + c_1$. From now on, let us put:

$$r = \alpha \frac{\log |\Delta|}{\log \log |\Delta|}, \quad \alpha \in [0, c_2] \tag{8}$$

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 3.3 *Notice that in proving Theorem 2.1 we can suppose, without loss of generality,*

$$B \geq H(E) \geq max\{c_{11}, e^3\}. \tag{9}$$

The first inequality because if $B < H(E)$ then $N(B) \leq N(H(E))$ and they have the same lower bound in the statement; the second (we need $M \geq e^3$ to ensure that $\log \log M > 0$ so that we have a meaningful upper bound in the RHS of (4), and we will need $B > c_{11}$ in Section 4) because there is only a finite number of elliptic curves with $H(E) < max\{c_{11}, e^3\}$.

In what follows, E will be an elliptic curve as in (2), with no further hyphoteses on the torsion.

4 Main argument

The following argument is due to Bombieri and Zannier and can be found, presented in similar fashion, in [1].
Our strategy is simple:

1. we find a small enough radius ρ_0 such that we can bound the number of points of the lattice in a ball of radius ρ_0 centered at a point of the lattice;
2. we count how many of this balls we need to cover all the lattice inside the ball of centre 0 and radius $\sqrt{\log B}$.

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

Lemma 4.1 *Given a positive integer n, radii R, ρ and a subset S of the n-ball $B(0,R)$, 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 $\mathcal{B}(0, R+\frac{\rho}{2})$, which gives $|\Gamma| \leq \frac{V_n(R+\frac{\rho}{2})}{V_n(\frac{\rho}{2})} \leq (1+\frac{2R}{\rho})^n$ 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. □

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.

For the first step, we need to distinguish two cases: small and large rank.

Small rank: in this case, we use a result by Masser, which can be found in [4]:

Theorem 4.2 *There exist a constant $c_3 > 1$ such that the number of rational points of E with canonical height bounded by $\frac{1}{C}$ is at most $Ch(E)^{\frac{3}{2}}$.*

So using Lemma 4.1 with $\rho = C^{-\frac{1}{2}}$ we find:

$$N(B) \leq |T|Ch(E)^{\frac{3}{2}}(1+2RC^{\frac{1}{2}})^r \leq (c_4 \log B)^{\frac{3}{2}}(c_5\sqrt{\log B})^r \leq (c_6 \log B)^{\frac{r+3}{2}}.$$

Along with (5), Lemma 3.2 and (9) this gives:

$$N(B) \leq (\log B)^{c_7\alpha\frac{\log B}{\log\log B}} = B^{c_7\alpha}$$

which implies our desired result for, for example, $\alpha \leq \frac{1}{\sqrt{\log B}}$.

Large rank: in this case we employ a result of Petsche concerning the *minimum canonical height* of a non torsion point. It turns out that this quantity can be bounded below as a function of the minimal discriminant Δ_m of the curve and of its *Szpiro ratio*:

$$\sigma = \frac{\log|\Delta_m|}{\log \mathcal{N}} \tag{10}$$

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

Theorem 4.3 *There exists a constant c_8 such that for any non-torsion point $P \in E(\mathbb{Q})$, we have*

$$\hat{h}(P) > \frac{\log|\Delta_m|}{c_8\sigma^6}$$

Proof: We recall for the reader's convenience Prop. 7 of [5]:

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 LHS of (25) is precisely 0 since $\mathbb{Q}$ has just one archimedean place, and no estimate is needed. This enables us to remove the $\log{(c_2 d\sigma^2)}$ factor in the statement. The rest of the proof is the same as the original. □

Remark 4.4 *Actually, this refinement is not really needed for our purposes, because, since $\sigma \geq 1$, we can "absorb" the aforementioned* log *factor in the σ^2 factor by changing constant and write σ^3 instead. This exponent change, as will be easy to see, only results in a change of the absolute constant in the statement of Theorem 2.1. Nevertheless, it is interesting to see that we can slightly improve the bound for the smallest canonical height for $k = \mathbb{Q}$ (and even for imaginary quadratic fields).*

Since $\mathcal{N}$ is divisible by all the primes dividing Δ_m except at most 2 and 3, the rank being "large" (in the sense of (8)) means that the discriminant has a lot of prime divisors with small exponent, so the *Szpiro ratio* is not too small (it is always greater than 1, see []) and our lower bound will be good.
Let us formalize this line of reasoning: apply Lemma 4.1 with $\rho = \sqrt{\frac{\log|\Delta_m|}{c_8\sigma^6}}$: then we know that in each of these balls there is just 1 non-torsion point and so we obtain:

$$N(B) \leq \left(c_9\sqrt{\frac{\log B}{\log|\Delta|}}\sigma^3\right)^r \leq \left(c_9\frac{\log B}{log\mathcal{N}}\sigma^2\right)^{\alpha\frac{\log B}{\log\log B}}. \tag{11}$$

But from what we said earlier about the primes dividing $\mathcal{N}$, it follows that $6\mathcal{N}$ has at least $max\{2, \frac{r-2}{2}\} \geq \frac{r}{3}$ prime factors and hence

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

with $p_n\# := \prod_{j=1}^n p_j$ the primorial;
again by PNT we have $p_n\# = e^{(1+o(1))n\log n}$, which gives us:

$$\log 6 + \log\mathcal{N} \geq c_{10}\alpha\frac{\log B}{3\log\log B}(\log\alpha + \log\log B - \log\log\log B - \log\frac{c_{10}}{3})$$

and if $\alpha > \frac{1}{\sqrt{\log B}}$ then it follows that, for $B > c_{11}$,

$$\log\mathcal{N} \geq c_{12}\alpha\log B. \tag{12}$$

By (5) and (9), this immediately gives us:

$$\sigma \leq \frac{c_{13}}{\alpha} \tag{13}$$

Substituting (12) and (13) in (11) we get:

$$N(B) \leq B^{\frac{3\alpha \log\left(\frac{c_{13}}{\alpha}\right)}{\log\log B}} \tag{14}$$

It is elementary that the function $x \log\left(\frac{c_{13}}{x}\right)$ is bounded by an absolute constant in $[\frac{1}{\sqrt{\log B}}, \infty)$ (it is, in fact, bounded by $\frac{c_{13}}{e}$ on all $(0, \infty)$) and so we obtain:

$$N(B) \leq B^{\frac{c_{14}}{\log\log B}}$$

which concludes the proof of Theorem 2.1.

References

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

[2] H.G. Zimmer. On the difference of the weil height and the neron-tate height. 1976.

[3] J. H. Silverman e J. T. Tate. *Rational Points on Elliptic Curves*. Springer, pp. 80-98, 2015.

[4] D.W. Masser. Counting points of small height on elliptic curves. 1989.

[5] C. Petsche. Small rational points on elliptic curves over number fields. 2006.