ON THE TYPICAL RANK OF ELLIPTIC CURVES OVER $\mathbb{Q}(T)$

FRANCESCO BATTISTONI, SANDRO BETTIN, AND CHRISTOPHE DELAUNAY

ABSTRACT. As an application of Turán sieve, we give upper bounds for the number of elliptic curves defined over $\mathbb{Q}(T)$ in some families having positive rank, obtaining in particular that these form a subset of density zero. This confirms Cowan's conjecture [Cow20] in the case $m, n \leq 2$.

1. INTRODUCTION

Let $\mathcal{E}$ be an elliptic curve defined over $\mathbb{Q}(T)$ given by a Weierstrass equation

$$(1.1) \qquad \mathcal{E}: \quad Y^2 = X^3 + \alpha_2(T)X^2 + \alpha_4(T)X + \alpha_6(T),$$

where $\alpha_2(T), \alpha_4(T)$ and $\alpha_6(T)$ are polynomials in, say, $\mathbb{Z}[T]$. Since $\mathcal{E}$ is an elliptic curve, it has to be non-singular meaning that the discriminant of equation (1.1) is not 0 as a polynomial. Furthermore, we say that $\mathcal{E}$ is iso-trivial if the j-invariant associated to (1.1) is a constant rational function in $\mathbb{Q}(T)$. The group of $\mathbb{Q}(T)$-rational points of $\mathcal{E}$ is finitely generated and we denote by $r_{\mathcal{E}}$ the rank of $\mathcal{E}(\mathbb{Q}(T))$. The rank $r_{\mathcal{E}}$ is an important arithmetical invariant of elliptic curves over $\mathbb{Q}(T)$ and is related to several questions in number theory. For example, Silverman's specialization theorem asserts that for almost all specializations of T at $t \in \mathbb{Q}$, the rank of the associated elliptic curve defined over $\mathbb{Q}$ is at least $r_{\mathcal{E}}$. This has direct consequences on the study of the distribution of ranks of families of elliptic curves defined over $\mathbb{Q}$, or over number fields K [Mil06, DHP15, ST95, RS01] and on the research of high rank elliptic curves [Mes91, Fer97, ALRM07]. The study of the rank, $r_{\mathcal{E}}$, has also some impact on a question in arithmetic geometry asking whether the set of $\mathbb{Q}$-rational points of equation (1.1) seen as an hypersurface in the three dimensional affine space over $\mathbb{Q}$ is Zariski-dense. The question is positively answered whenever $r_{\mathcal{E}} > 0$, and if $r_{\mathcal{E}} = 0$ a sufficient criterion consists in showing that there exist infinitely many specializations of T at $t \in \mathbb{Q}$ such that the rank of the corresponding curve over $\mathbb{Q}$ is positive (see [Maz92] and recent works by J. Desjardins on the subject, [Des19a, Des18]). Under the parity conjecture this can be done, for example, by studying the behavior of the root numbers of the specializations.

In a recent work [Cow20], Cowan considered the typical value of $r_{\mathcal{E}}$, giving an heuristic argument suggesting that for most natural families of elliptic curves over $\mathbb{Q}(T)$ the rank $r_{\mathcal{E}}$ is zero for almost all member of the family. More specifically, letting $\|P\|$ be the absolute height[1] of a polynomial $P \in \mathbb{Z}[X]$ (i.e. the maximum of the absolute values of the coefficients of P), and writing for any $m, n, H \in \mathbb{N}$

$$\mathcal{S}_{m,n} := \{\mathcal{E} \mid \alpha_2 = 0, \ \deg(\alpha_4) \leq m, \ \deg(\alpha_6) \leq n, \ \mathcal{E} \text{ non-singular}\},$$

$$\mathcal{S}_{m,n}(H) := \{\mathcal{E} \in \mathcal{F}_{m,n} \mid \|\alpha_4\| < H^3, \ \|\alpha_6\| < H^2\},$$

he made the following conjecture.

---

[1]Cowan stated the conjecture for the Mahler measure μ, mentioning that one could also choose the height instead. By the inequalities $\binom{n}{[n/2]}^{-1}\|P\| \leq \mu(P) \leq \sqrt{n+1}\|P\|$ for P of degree n (see [BG06, Lemma 1.6.7]) the two choices are equivalent.

Conjecture 1. *Let $m, n \in \mathbb{N}$. Then, as $H \to \infty$ we have*

$$(1.2) \qquad \lim_{H \to \infty} \frac{1}{\sharp \mathcal{S}_{m,n}(H)} \sum_{\mathcal{E} \in \mathcal{S}_{m,n}(H)} r_{\mathcal{E}} = 0.$$

In particular,

$$(1.3) \qquad \lim_{H \to \infty} \frac{\sharp \{\mathcal{E} \in \mathcal{S}_{m,n}(H) \mid r_{\mathcal{E}} \geq 1\}}{\sharp \mathcal{S}_{m,n}(H)} = 0,$$

that is almost all elliptic curves defined over $\mathbb{Q}(T)$ have rank zero.

Notice that this conjecture is in contrast with what is expected to hold for elliptic curves over $\mathbb{Q}$. Indeed, considerations on the root numbers lead to the belief that for most natural families of elliptic curves over $\mathbb{Q}$ one has that 50% of the curves have rank 1 and 50% have rank 0. See for example [Gol79] for the case of quadratic twists and see [BDD18] for the study of some exceptional families.

In this note we use the results of [BBD21] to prove Cowan's conjecture in the case $m, n \leq 2$. Notice that in this case the elliptic surfaces defined by (1.1) over $\mathbb{P}^1_{\mathbb{Q}}$ are all rational elliptic surfaces since $\deg(\alpha_i) \leq i$ and, with $m, n \leq 2$, the discriminant of $\mathcal{E}$ can not be a constant time the twelfth power of a degree one polynomial (cf. [SS10]). Rational elliptic surfaces over $\mathbb{P}^1_{\mathbb{Q}}$ are the ones with a geometric genus, $g_{\mathcal{E}}$, equal to zero leading to the simplest geometry and an easier control of the Mordell-Weil rank over $\mathbb{Q}(T)$ of the associated elliptic curve. More precisely, we obtain the following result.

Theorem 1. *Conjecture 1 holds for $1 \leq m, n \leq 2$.*

We also consider the problem for other families of elliptic curves over $\mathbb{Q}(T)$, where α_2 is not required to be zero. In the case of $\deg(\alpha_i) \leq 2$ for $i = 2, 4, 6$, we can rewrite the right hand side of (1.1) as a polynomial in T, writing $\mathcal{E} = \mathcal{E}_{A,B,C}$ as

$$(1.4) \qquad \mathcal{E}_{A,B,C}: \quad Y^2 = A(X)T^2 + B(X)T + C(X)$$

where $A(X), B(X)$ and $C(X) - X^3$ are polynomials in $\mathbb{Z}[X]$ of degree ≤ 2. For $P_1, \ldots, P_n \in \mathbb{Z}[X]$ we let $\|P_1, \ldots, P_n\| := \max(\|P_1\|, \ldots, \|P_n\|)$. We shall consider the following 3 families, the last one being different from $\mathcal{S}_{2,2}(H)$ only for the different ordering.[2]

$\mathcal{S}_0(H) := \{\mathcal{E}_{A,B,C} \mid A = 0, \ \deg(B), \deg(C - X^3) \leq 2, \ \|B, C\| \leq H, \ \mathcal{E} \text{ non-singular}\},$

$\mathcal{S}_\square(H) := \{\mathcal{E}_{A^2,B,C} \mid \deg(A) = 0, \ \deg(B), \deg(C - X^3) \leq 2, \ \|A, B, C\| \leq H, \ \mathcal{E} \text{ non-singular}\},$

$\mathcal{S}_\ell(H) := \{\mathcal{E}_{A,B,C} \mid \deg(A), \deg(B), \deg(C - X^3) \leq 1, \ \|A, B, C\| \leq H, \ \mathcal{E} \text{ non-singular}\}.$

Notice that the case $\mathcal{S}_0$ corresponds to elliptic curves defined by (1.1) with $\deg(\alpha_2) \leq 1$, $\deg(\alpha_4) \leq 1$ and $\deg(\alpha_6) \leq 1$. The case $\mathcal{S}_\square$ corresponds to (1.1) with $\deg(\alpha_2) \leq 1$, $\deg(\alpha_4) \leq 1$ and α_6 of degree 2 with a square leading coefficient. Finally, the case $\mathcal{S}_\ell$ corresponds to (1.1) with $\alpha_2(T) = 0$ and $\deg \alpha_4(T) \leq 2$, $\deg \alpha_6(T) \leq 2$. The elliptic curves in all of these families have rank bounded by 5 over $\mathbb{Q}(T)$ (cf. [BBD21]) whenever the elliptic curve is non-isotrivial. In our case ($\deg A, \deg B \leq 2$), it is not difficult to see that $\mathcal{E}_{A,B,C}$ is iso-trivial if and only if $A = B = 0$ (this is not true in general for elliptic curves over $\mathbb{Q}(T)$). In particular, the contribution of isotrivial cases can be easily bounded by [BS15] (see Section 3) and we have that the analogous of (1.2) and (1.3) are equivalent in our case.

Also for these families we can show that almost all elliptic curves have rank zero over $\mathbb{Q}(T)$.

---

[2]It would be possible to use alternative orderings also for these families.

Theorem 2. *For any $* \in \{0, \square, \ell\}$ let $\mathcal{R}_*(H) := \{\mathcal{E}_{A,B,C} \in \mathcal{S}_*(H) \mid r_{\mathcal{E}_{A,B,C}} \geq 1\}$. Then,*

$$(1.5) \qquad \lim_{H \to \infty} \frac{\sharp \mathcal{R}_*(H)}{\sharp \mathcal{S}_*(H)} = 0.$$

Remark 1. *Our method is based on a simple application of the Turán sieve and actually gives quantitative bounds. In particular for Theorem 2 we show that*

$$\frac{\sharp \mathcal{R}_*(H)}{\sharp \mathcal{S}_*(H)} = O(H^{-1/3}(\log H \log \log H)^{2/3}).$$

The application of an Hilbert's irreducibility argument could have been an alternative tool for proving the main theorem. In particular, the result Castillo and Dietmann ([CD17]) should very likely produce a better error term.

Remark 2. *One of the key ingredient is Theorem 3, which is not expected to generalize to the case of α_2, α_4 and α_6 with degree large enough, in particular whenever the underlying elliptic surface is a K3 surface. However, it seems natural to expect a zero density result in this case too, as explained by Cowan ([Cow20]).*

Remark 3. *Note that, during the refereeing process of this paper, Remke Kloosterman ([Klo22]) announced the proof of the full Cowan's conjecture (and a generalization of it) by a different method.*

Conjecture 1 and Theorems 1 and 2 suggest that the rank over $\mathbb{Q}(T)$ of elliptic curves is typically expected to be zero. Thus, the study of the Zariski density of $\mathbb{Q}$-rational points of (1.1) seen in the affine three space cannot, in general, be addressed by rank considerations only. However, in general the root number should be, under the Chowla and squarefree conjectures, equidistributed and hence there should exist infinitely many specializations with rank ≥ 1 over $\mathbb{Q}$, implying (conditionally) the Zariski density (see [Hel09, Des19b]). This strategy does not apply whenever the root number is not equidistributed: this happens to be the case for potentially parity biased families as studied in [BDD18], where it is proved that there are essentially 6 different classes of such non-isotrivial families of the form (1.1) with $\deg(\alpha_2), \deg(\alpha_4), \deg(\alpha_6) \leq 2$. Among those 6 classes, two correspond to the families considered in this paper. These are

$$\mathcal{E}: \quad wY^2 = X^3 + 3TX^2 + 3sX + sT \quad (* = 0)$$
$$\mathcal{G}: \quad Y^2 = X^3 + 3TX^2 + 3TX + T^2 \quad (* = \square)$$

It is proved unconditionally in [Des18] that the family $\mathcal{G}$ has infinitely many integer specializations with negative root number. In [CD20], the authors investigate, in particular, the situation given by (sub)-families of $\mathcal{E}$ and describe the possibilities to have families with constant root number.

The organization of the paper is the following. In Section 2 we give some lemmas which we will need in the proofs. Among these, we mention in particular the main ingredient, Theorem 3, that we deduce directly from [BBD21] and which shows that it suffices to bound the number of reducible polynomials in certain sets. In Section 3, we prove Theorem 2 by showing how to obtain such bounds as a consequence of the Turán sieve. In Section 4 we show how the same proof can be adapted (and in fact simplified) to prove Theorem 1.

GNAMPA and his work is partially supported by PRIN 2017 "Geometric, algebraic and analytic methods in arithmetic".

2. PRELIMINARIES

We start with the following standard application of the Turán sieve. We include a proof for the sake of completeness.

Lemma 1. *Let $f(a_1, \cdots, a_n, X) \in \mathbb{Z}[a_1, \cdots, a_n][X]$ with $n > 1$. Let $\mathcal{P}$ be a set of primes such that $\mathcal{P} \cap [1, x] \sim C \frac{x}{\log x}$ as $x \to \infty$ for some $C > 0$. Assume there exists $\delta > 0$ such that for all $p \in \mathcal{P}$ the set*

$$\mathcal{A}_p = \{(a_1, \cdots, a_n) \in \mathbb{F}_p^n \mid f(a_1, \cdots, a_n, X) \text{ is irreducible in } \mathbb{F}_p[X]\}$$

satisfies $\sharp \mathcal{A}_p = \frac{p^n}{\delta} + O(p^{n-1})$ as $p \to \infty$. Finally, for $\boldsymbol{H} = (H_1, \ldots, H_n) \in \mathbb{R}_{>0}^n$, let

$$\mathcal{B}(\boldsymbol{H}) := \{(a_1, \cdots, a_n) \in \mathbb{Z}^n \mid |a_i| \leq H_i \; \forall i \text{ and } f(a_1, \cdots, a_n, X) \text{ is reducible in } \mathbb{Q}[X]\}.$$

Then, letting $H := \min(H_1, \ldots, H_n)$, as $H \to \infty$ we have

$$\sharp \mathcal{B}(\boldsymbol{H}) \ll H_1 \cdots H_n \cdot H^{-1/3} (\log H \log \log H)^{2/3}.$$

Proof. For all $p \in \mathcal{P}$, we define

$$\mathcal{A}_p(\boldsymbol{H}) = \{(a_1, \cdots, a_n) \in \mathbb{Z}^n \mid |a_i| \leq H_i \; \forall i \text{ and } f(a_1, \cdots, a_n, X) \text{ is irreducible in } \mathbb{F}_p[X]\}.$$

Let $X := H_1 \cdots H_n$. If $p \leq H$, $p \in \mathcal{P}$, then we have

$$\sharp \mathcal{A}_p(\boldsymbol{H}) = \frac{X}{p^n} \Big(1 + O\Big(\frac{p}{H}\Big)\Big) \sharp \mathcal{A}_p = \frac{X}{\delta} + O\Big(\frac{X}{p}\Big) + O(pX/H) = \frac{X}{\delta} + R_p,$$

say. Moreover, by the Chinese Remainder Theorem, if $p, q \in \mathcal{P}$ satisfy $p, q \leq H^{1/2}$, then

$$\sharp(\mathcal{A}_p(H) \cap \mathcal{A}_q(H)) = \frac{X}{(pq)^n} \Big(1 + O\Big(\frac{pq}{H}\Big)\Big) \sharp \mathcal{A}_p \sharp \mathcal{A}_q$$

$$= \frac{X}{\delta^2} + O\Big(\frac{X}{p}\Big) + O\Big(\frac{X}{q}\Big) + O(pqX/H) = \frac{X}{\delta^2} + R_{p,q},$$

say. Now we define

$$\mathcal{B}_{\mathcal{P},z}(\boldsymbol{H}) = \{(a_1, \cdots, a_n) \in \mathbb{Z}^n \mid |a_i| \leq H_i \; \forall i \text{ and } f(a_1, \cdots, a_n, X)$$
$$\text{is reducible in } \mathbb{F}_p[X] \text{ for all } p \in \mathcal{P} \text{ with } p \leq z\}$$

and we apply Turán's sieve [CM06, chapter 4], which gives that for $z \leq H^{1/2}$

$$\sharp \mathcal{B}_{\mathcal{P},z}(\boldsymbol{H}) \leq \frac{H^n}{\sum_{\substack{p \in \mathcal{P} \\ p \leq z}} \delta} + \frac{2}{\sum_{\substack{p \in \mathcal{P} \\ p \leq z}} \delta} \sum_{\substack{p \in \mathcal{P} \\ p \leq z}} |R_p| + \frac{1}{(\sum_{\substack{p \in \mathcal{P} \\ p \leq z}} \delta)^2} \sum_{\substack{p,q \in \mathcal{P} \\ p,q \leq z}} |R_{p,q}|$$

$$\ll X \frac{\log z}{z} + X \frac{\log z \log \log z}{z} + zX/H + z^2 X/H$$

$$\ll XH^{-1/3} (\log H \log \log H)^{2/3},$$

upon choosing $z = (H \log H \log \log H)^{1/3}$. The lemma then follows since $\sharp \mathcal{B}(\boldsymbol{H}) \leq \sharp \mathcal{B}_{\mathcal{P},z}(\boldsymbol{H})$. $\square$

When applying this lemma to our cases, we will need some results on the number of irreducible polynomials in $\mathbb{F}_p[x]$ satisfying certain properties.

Lemma 2. *Let q be a prime power. The number of irreducible, monic polynomials of degree $n \geq 1$ is $\frac{1}{n} \sum_{d|n} \mu(d) q^{\frac{n}{d}}$, where μ denotes the Möbius function.*

Proof. See e.g. [Ros02, Corollary of Proposition 2.1]. □

Lemma 3. *Let q be an odd prime power. The number of even, irreducible, monic polynomials of degree $n \geq 4$ is $\frac{1}{n} \sum_{\substack{d \mid n \\ d \text{ odd}}} \mu(d)(q^{\frac{n}{2d}} - 1)$.*

Proof. See [Coh68, Theorem 3]. □

Lemma 4. *Let q be an odd prime power, $a \in \mathbb{F}_q$, and $n \geq 4$ even. The number of even, irreducible, monic polynomials of degree n such that the coefficient of the x^{n-2} term is a is $\frac{1}{n} q^{n/2-1} + O(q^{n/4})$.*

Proof. By [Coh68, Theorem 2] we have that the set of polynomials satisfying the above conditions is in bijection with

$$S_a := \{P \in \mathbb{F}_q[x] \mid P \text{ monic irreducible}, \deg(P) = n', P_{n'-1} = a, (-1)^{n'} P_0 \text{ non-square mod } q\},$$

where $n' = n/2$, P_i is the i-th coefficient of $P(X)$ and where we used the fact that the condition of $(-1)^{n'} P_0$ (non-zero) being a non-square modulo q is equivalent to $(2, (q-1)/e) = 1$ with e the order of $(-1)^{n'} P_0$ modulo q. The lemma then follows since Theorem 2 in [Car52] gives an exact formula for the cardinality of S_a, implying in particular that $|S_a| = \frac{1}{n} q^{n/2-1} + O(q^{n/4})$. □

Finally, we give some bounds for the rank which follow immediately from [BBD21]. We need the following definition

$$M_{P_1,P_2}(X) := \operatorname*{Res}_Y(P_1(Y), X^2 - P_2(Y))$$

for two polynomials $P_1, P_2 \in \mathbb{Z}[X]$, with $P_2 \neq 0$, where the resultant is computed with respect to the variable Y. Also, given a polynomial $P \in \mathbb{Z}[X] \setminus \{0\}$, we denote by $\Omega(P)$ the number of irreducible factors of P counted with multiplicity.

Theorem 3. *Let $\mathcal{E}_{A,B,C}$ as in (1.4) with $\deg(A), \deg(B) \leq 2$ and C monic of degree 3. Also assume A and B are not both zero. Then $r_{\mathcal{E}_{A,B,C}} \leq 5$. Moreover,*

$$r_{\mathcal{E}_{A,B,C}} \leq \begin{cases} \Omega(M_{B,C}) - 1 & \text{if } A = 0, \\ \Omega(B^2 - 4AC) - 1 & \text{if } A \in \mathbb{Z}^2_{\neq 0}, \text{ or if } A \in \mathbb{Z} \text{ and } \deg(B) \leq 1 \\ \Omega(M_{B^2-4AC,A}) - 1 & \text{if } \deg(A) = 1. \end{cases}$$

Proof. A formula for the rank valid for $\deg(A), \deg(B), \deg(C - X^3) \leq 2$ is given in [BBD21, Theorem 1]. The claimed inequalities then follow easily. We only remark that in the case $A \in \mathbb{Z} \setminus \mathbb{Z}^2$ and $\deg(B) \leq 1$, [BBD21] gives that $r_{\mathcal{E}_{A,B,C}}$ is the number of conjugate classes of roots ρ of $B^2 - 4AC$ such that A is a square in $\mathbb{Q}(\rho)$. Since $B^2 - 4AC$ has degree 3, then such a number is zero unless $B^2 - 4AC$ has an irreducible factor of degree 2 and the claimed inequality follows. □

3. Proof of Theorem 2

In this section we prove that (1.5) holds for the three families considered. We remark that this implies also that the average rank is zero. Indeed, since for A, B not both zero we have $r \leq 5$ by Theorem 3, it is sufficient to bound the contribution from $A = B = 0$: recall that in our situation, $A = B = 0$ correspond exactly to the isotrivial case. These iso-trivial families are perhaps most naturally excluded from the definition of the average rank. In any case, one can bound their contribution by [BS15], since for H sufficiently large we have the very crude bound

$$\sideset{}{^*}\sum_{\substack{\deg(C-X^3) \leq 2 \\ \|C\| \leq H}} r_{\mathcal{E}_{0,0,C}} \leq 2 \sideset{}{^*}\sum_{|c_0| \leq 55H^3, |c_1| \leq 28H^2} r_{\mathcal{E}_{0,0,X^3+c_1X+c_0}} \ll H^5$$

which is sufficient for our purposes, where $\sum^*$ indicates that singular curves are to be excluded from the sum.

3.1. The case $* = 0$.
By Theorem 3 it suffices to show that almost all polynomials $B, C \in \mathbb{Z}[X]$ with $\deg(B), \deg(C - X^3) \leq 2$ are such that $M_{B,C}$ is irreducible. We let $B(X) = b_2 X^2 + b_1 X + b_0$ and $C(X) = X^3 + c_2 X^2 + c_1 X + c_0$. Then,

$$M_{B,C}(X) = b_2^3 X^4 + \left(-2c_0 b_2^3 + (c_1 b_1 + 2c_2 b_0)b_2^2 + (-c_2 b_1^2 - 3b_0 b_1)b_2 + b_1^3 \right) X^2 +$$
$$+ c_0^2 b_2^3 + \left(-c_0 c_1 b_1 + (-2c_0 c_2 + c_1^2)b_0 \right)b_2^2 + \left(c_0 c_2 b_1^2 + (-c_1 c_2 + 3c_0)b_0 b_1 + \right.$$
$$\left. + (c_2^2 - 2c_1)b_0^2 \right)b_2 + (-c_0 b_1^3 + c_1 b_0 b_1^2 - c_2 b_0^2 b_1 + b_0^3).$$

Given an irreducible $U(X) = u_4 X^4 + u_2 X^2 + u_0 \in \mathbb{F}_p[X]$ and a prime $p \geq 5$ we need to count the number $\mathcal{N}_U$ of $(b_2, b_1, b_0, c_2, c_1, c_0) \in \mathbb{F}_p[x]^6$ such that $M_{B,C}(X) \equiv U(X) \mod p$, i.e.

$$(3.1) \quad \begin{cases} b_2^3 & \equiv u_4, \\ \left(-2c_0 b_2^3 + (c_1 b_1 + 2c_2 b_0)b_2^2 + (-c_2 b_1^2 - 3b_0 b_1)b_2 + b_1^3 \right) & \equiv u_2, \\ c_0^2 b_2^3 + \left(-c_0 c_1 b_1 + (-2c_0 c_2 + c_1^2)b_0 \right)b_2^2 + \left(c_0 c_2 b_1^2 + (-c_1 c_2 + 3c_0)b_0 b_1 + \right. \\ \left. + (c_2^2 - 2c_1)b_0^2 \right)b_2 + (-c_0 b_1^3 + c_1 b_0 b_1^2 - c_2 b_0^2 b_1 + b_0^3). & \equiv u_0. \end{cases}$$

It is convenient to assume $p \equiv 2 \mod 3$ so that the cubic map is an automorphism of $\mathbb{F}_p$. If $u_4 \equiv 0$, then one easily sees that the system has $\mathcal{N}_U = p^3$ solutions. If $u_4 \not\equiv 0$, then the first two equations determine unique values for b_2 and c_0 respectively. Inserting these values in the third equation, this reduces to

$$\Delta_B b_2^4 \left(c_1 + \frac{3b_1^2 - 4b_1 b_2 c_2 + \Delta_B}{4b_2^2} \right)^2 \equiv \tilde{\Delta}_U,$$

where $\Delta_B := b_1^2 - 4b_0 b_2$ and $\tilde{\Delta}_U := u_2^2 - 4u_0 u_4$ and for some (non-zero) b_2 determined by u_4. Since $\tilde{\Delta}_U \not\equiv 0$, this equation has two solutions in c_1 if $\tilde{\Delta}_U \Delta_B$ is a non-zero square modulo p and no solutions otherwise. Denoting the Legendre symbol by $(\frac{\cdot}{\cdot})$ we obtain

$$\mathcal{N}_U = \sum_{b_0, b_1, c_2 \bmod p} \left(\left(\frac{\Delta_B^2}{p} \right) + \left(\frac{\tilde{\Delta}_U \Delta_B}{p} \right) \right) = p \sum_{b_0, b_1 \bmod p} \left(\left(\frac{\Delta_B^2}{p} \right) + \left(\frac{\tilde{\Delta}_U \Delta_B}{p} \right) \right) = p^3 - p^2.$$

Thus, letting $\mathcal{A}_p := \{(b_2, b_1, b_0, c_2, c_1, c_0) \in \mathbb{F}_p^6 \mid M_{B,C}(X) \text{ is irreducible in } \mathbb{F}_p[X]\}$, we have

$$\sharp \mathcal{A}_p = \sum_{\substack{U \in \mathbb{F}_p[X], \deg U \leq 4 \\ U \text{ even, irreducible}}} \mathcal{N}_U = \sum_{\substack{U \in \mathbb{F}_p[X], \deg U = 4 \\ U \text{ even, irreducible}}} p^3 + O(p^5), = \frac{p^6}{4} + O(p^5)$$

by Lemma 3. Thus, we obtain the theorem in the case $* = 0$ (and error as given in Remark 1) by applying Lemma 1 with $\mathcal{P} = \{p \equiv 2 \mod 3\}$ (so that $C = 1/2$) and $H_1 = \cdots = H_6 = H$.

3.2. The case $* = \square$.
By Theorem 3 it suffices to show that almost all polynomials $A \in \mathbb{Z}$, $B, C \in \mathbb{Z}[X]$ with $\deg(B), \deg(C - X^3) \leq 2$ are such that $B^2 - 4A^2 C$ is irreducible. We let B and C as in the previous subsection and $A = k$. We have

$$B(X)^2 - 4A^2 C(X) = b_2^2 X^4 + (2b_1 b_2 - 4k^2)X^3 + (2b_0 b_2 + (b_1^2 - 4k^2 c_2))X^2 +$$
$$+ (2b_0 b_1 - 4k^2 c_1)X + (b_0^2 - 4k^2 c_0).$$

Given a prime $p \geq 3$ and any $U(X) = u_4 X^4 + \cdots + u_0 \in \mathbb{F}_p[X]$ irreducible, we need to find the number of solutions $\mathcal{N}_p$ to $B^2 - 4A^2C \equiv U$, i.e. the number of solutions to

(3.2)
$$
\begin{cases}
b_2^2 & \equiv u_4, \\
2b_1 b_2 - 4k^2 & \equiv u_3, \\
2b_0 b_2 + (b_1^2 - 4k^2 c_2) & \equiv u_2, \\
2b_0 b_1 - 4k^2 c_1 & \equiv u_1, \\
b_0^2 - 4k^2 c_0 & \equiv u_0.
\end{cases}
$$

First notice that we can assume $k \not\equiv 0$ since otherwise $B^2 - 4k^2 C$ cannot be irreducible. If $u_4 \equiv 0$, we have $b_2 \equiv 0$ and we then obtain $(1 + (\frac{u_3}{p}))$ choices for k. Choosing among the p^2 possibilities for the couple (b_1, b_0) the remaining variables c_2, c_1 and c_0 are uniquely determined and thus $\mathcal{N}_U = (1 + (\frac{u_3}{p}))p^2$.

If $u_4 \not\equiv 0$, we have $(1 + (\frac{u_4}{p}))$ choices for b_2. Each of these give $(1 + (\frac{2b_1 b_2 - u_3}{p}))$ possible choices for k. Since c_2, c_1 and c_0 are uniquely determined by the other variables we thus obtain

$$
\mathcal{N}_p = \sum_{b_1, b_2 \bmod p} \left(1 + \left(\frac{u_4}{p}\right)\right)\left(1 + \left(\frac{2b_1 b_2 - u_3}{p}\right)\right) = \left(1 + \left(\frac{u_4}{p}\right)\right)\left(p^2 - p + p\left(\frac{-u_3}{p}\right)\right).
$$

Thus, for $\mathcal{A}_p := \{(k, b_2, b_1, b_0, c_2, c_1, c_0) \in \mathbb{F}_p^7 \mid B^2 - 4A^2C \text{ is irreducible in } \mathbb{F}_p[X]\}$ we have

$$
\sharp \mathcal{A}_p = \sum_{\substack{U \in \mathbb{F}_p[X] \text{ irreducible} \\ \deg U \leq 4}} \mathcal{N}_U = \sum_{\substack{U \in \mathbb{F}_p[X] \text{ irreducible} \\ \deg U = 4}} \left(1 + \left(\frac{u_4}{p}\right)\right)p + O(p^6)
$$

$$
= p^2 \sum_{\substack{U \in \mathbb{F}_p[X] \text{ irreducible} \\ \deg U = 4}} 1 + O(p^6) = \frac{p^7}{4} + O(p^6),
$$

by Lemma 2. The theorem in this case then follows as before.

Remark 4. *It would be interesting to have the result also in the case with A in place of A^2. In this case the rank is the number of conjugate classes of roots ρ of $B^2 - 4AC$ such that A is a square in $\mathbb{Q}(\rho)$. In order to show this number is typically zero one would need to prove that the resolvent cubic of $B^2 - 4kC$ is almost always irreducible.*

3.3. **The case $* = \ell$.** By Theorem 3 it suffices to show that almost all polynomials $A, B, C \in \mathbb{Z}[X]$ with $\deg(A), \deg(B), \deg(C - X^3) \leq 1$ are such that $M_{B^2 - 4AC, A}$ is irreducible. We let $A(X) = a_1 x + a_0$, $B(X) = b_1 X + b_0$ and $C(X) = X^3 + c_1 X + c_0$. If $a_1 \not\equiv 0$, which we can assume at a cost of an admissible error, then

$$
a_1^{-1} M_{B^2 - 4AC, A}(X) = -4X^8 + 12a_0 X^6 + (-12a_0^2 + a_1 b_1^2 - 4a_1^2 c_1)X^4 + (4a_0^3 + 2a_1^2 b_0 b_1 +
$$
$$
- 2a_0 a_1 b_1^2 - 4a_1^3 c_0 + 4a_0 a_1^2 c_1)X^2 + (a_1^3 b_0^2 - 2a_0 a_1^2 b_0 b_1 + a_0^2 a_1 b_1^2).
$$

Let $p \geq 5$ be prime and $U(X) = -4X^8 + u_6 X^6 + \cdots + u_2 X^2 + u_0 \in \mathbb{F}_p[X]$ be even and irreducible. We have that $a_1^{-1} M_{B^2 - 4AC, A} \equiv U$ is equivalent to

(3.3)
$$
\begin{cases}
a_0 & \equiv u_6/12, \\
-12a_0^2 + a_1 b_1^2 - 4a_1^2 c_1 & \equiv u_4, \\
4a_0^3 + 2a_1^2 b_0 b_1 - 2a_0 a_1 b_1^2 - 4a_1^3 c_0 + 4a_0 a_1^2 c_1 & \equiv u_2, \\
a_1^3 b_0^2 - 2a_0 a_1^2 b_0 b_1 + a_0^2 a_1 b_1^2 & \equiv u_0.
\end{cases}
$$

Notice that we can't have $a_1 \equiv 0$ since the last equation would imply $u_0 \equiv 0$ which is not possible since U is irreducible. We then solve the second equation in c_1 inserting the result in the last two equations reducing them to

$$\begin{cases} c_0 & \equiv 4(432a_1^2 b_0 b_1 - 216u_2 - 18a_1 b_1^2 u_6 - 18u_4 u_6 - u_6^3)/(864a_1^3) \\ (b_0 - b_1 u_6/(12a_1))^2 & \equiv u_0/a_1^3. \end{cases}$$

The second equation implies that u_0/a_1 is a square modulo p, and so we have $(p-1)/2$ possible choices for a_1. For each of these and for any choice of b_1 we then have two possibilities for b_0, whereas c_0 is determined by the remaining variables. It follows that the above system has $p^2 - p$ solutions.

For $\mathcal{A}_p := \{(a_0, a_1, b_0, b_1, c_0, c_1) \in \mathbb{F}_p^6 \mid M_{B^2-4AC,A} \text{ is irreducible in } \mathbb{F}_p[X]\}$ we then have

$$\sharp \mathcal{A}_p = p^2 \sum_{\substack{U \in \mathbb{F}_p[X], \ \deg U = 8, \\ U \text{ monic, even, irreducible}}} \mathcal{N}_U + O(p^5) = \frac{p^6}{8} + O(p^5)$$

by Lemma 3. The theorem in this case then follows as before.

4. PROOF OF THEOREM 1

First, we observe that by the same argument given at the beginning of the previous section (which is not wasteful in this case), it suffices to prove (1.3).

The case of $m = n = 2$ is essentially identical to the case $* = \ell$ with the only difference of the different ordering which can be accounted for by choosing appropriately the H_i in Lemma 1.

The case of $m = n = 1$ corresponds to elliptic curves with $A = 0$, $\deg(B) \le 1$, $\deg(C - x^3) \le 1$. This is a simpler version of the case $* = 0$ as now we have $c_2 = b_2 = 0$ (and thus U has degree ≤ 2). Then, (3.1) reduces to

$$\begin{cases} b_1^3 & \equiv u_2, \\ -c_0 b_1^3 + c_1 b_0 b_1^2 + b_0^3 & \equiv u_0. \end{cases}$$

and one immediately sees that this system has p^2 solutions if $5 \le p \equiv 2 \mod 3$. There are $\frac{1}{2}p^2 + O(p)$ irreducible even quadratic polynomials U, since there are $(p-1)/2$ squares in $\mathbb{F}_p$, and so $M_{B,C}$ is irreducible mod p for $p^4/2 + O(p^3)$ choices of the parameters modulo p. The result then follows by Lemma 1.

The case of $m = 1, n = 2$ corresponds to elliptic curves with $\deg(A) = 0$, $\deg(B) \le 1$, $\deg(C - x^3) \le 1$, which is very similar to the case $* = \square$, with the difference that now we have A in place of A^2 (and thus k in place of k^2) and $c_2 = b_2 = 0$ (and thus U has degree ≤ 3). Thus, (3.2) becomes

$$\begin{cases} -4k & \equiv u_3, \\ b_1^2 & \equiv u_2, \\ 2b_0 b_1 - 4kc_1 & \equiv u_1, \\ b_0^2 - 4kc_0 & \equiv u_0. \end{cases}$$

This system has $(1 + (\frac{u_2}{p}))p$ solutions if $u_3 \not\equiv 0$, $O(p^2)$ solutions if $u_3 \equiv 0$ and $4u_0 u_2 \equiv u_1^2$, and $O(p)$ solutions if $u_3 \equiv 0$ and $4u_0 u_2 \not\equiv u_1^2$. It follows that the number of choices of the

parameters such that $B^2 - 4AC$ is irreducible modulo p is

$$\sum_{\substack{U \in \mathbb{F}_p[X] \text{ irred.} \\ \deg U \leq 4}} \left(1 + \left(\frac{u_3}{p}\right)\right) p + O(p^5) = \sum_{u_4 \bmod p} \sum_{\substack{U \in \mathbb{F}_p[X] \text{ irred. monic} \\ \deg U = 4}} \left(1 + \left(\frac{u_3 u_4}{p}\right)\right) p + O(p^5)$$

$$= \frac{p^6}{4} + O(p^5)$$

and the result follows.

Finally, the case of $m = 2, n = 1$ corresponds to elliptic curves with $A(X) = aX$, $a \in \mathbb{Z}$, $\deg(B) \leq 1$, $\deg(C - x^3) \leq 1$. This is analogous to the case $* = \ell$, with the difference that now we have $a_0 = 0$. Thus, for $U(X) = -4X^8 + u_6 X^6 + \cdots + u_0 \in \mathbb{F}_p[X]$ even and irreducible, the system (3.3) becomes

$$\begin{cases} 0 & \equiv u_6, \\ a_1 b_1^2 - 4a_1^2 c_1 & \equiv u_4, \\ 2a_1^2 b_0 b_1 - 4a_1^3 c_0 & \equiv u_2, \\ a_1^3 b_0^2 & \equiv u_0. \end{cases}$$

If $u_6 \equiv 0$ and $5 \leq p \equiv 2 \bmod 3$ this has $p^2 - p$ solutions. By Lemma 4 we then have that $M_{B^2-4AC,A}$ is irreducible for $\frac{1}{8}p^5 + O(p^4)$ choices of the parameters and the result follows.

DATA AVAILAIBILITY AND CONFLICT OF INTEREST

Data sharing not applicable to this article as no datasets were generated or analysed during the current study. This article does not involve any conflict of interest.

REFERENCES

[ALRM07] Scott Arms, Álvaro Lozano-Robledo, and Steven J. Miller. Constructing one-parameter families of elliptic curves with moderate rank. *J. Number Theory*, 123(2):388–402, 2007.

[BBD21] Francesco Battistoni, Sandro Bettin, and Christophe Delaunay. Ranks of elliptic curves over $\mathbb{Q}(T)$ of small degree in T. *Preprint, arXiv:2109.00738*, 2021.

[BDD18] Sandro Bettin, Chantal David, and Christophe Delaunay. Non-isotrivial elliptic surfaces with non-zero average root number. *J. Number Theory*, 191:1–84, 2018.

[BG06] Bombieri Enrico and Gubler Walter. Heights in Diophantine geometry. *New Mathematical Monographs*, 4, Cambridge University Press, Cambridge, 2006.

[BS15] Manjul Bhargava and Arul Shankar Binary quartic forms having bounded invariants, and the boundedness of the average rank of elliptic curves. *Ann. of Math.*, 181(1): 191–242, 2015.

[Car52] Leonard Carlitz. A theorem of Dickson on irreducible polynomials. *Proc. Amer. Math. Soc.* 3:693–700, 1952.

[CD17] Castillo Abel and Dietmann Rainer. On Hilbert's irreducibility theorem. *Acta Arith.* 180: 1–14, 2017.

[CD20] Rena Chu and Julie Desjardins. Constant root number on integer fibres of elliptic surfaces. *Preprint available at* https://arxiv.org/pdf/2011.02386.pdf, 2020.

[CM06] Alina Carmen Cojocaru and M. Ram Murty. *An introduction to sieve methods and their applications*, volume 66 of *London Mathematical Society Student Texts*. Cambridge University Press, Cambridge, 2006.

[Coh68] Stephen D. Cohen. On irreducible polynomials of certain types in finite fields. *Math. Proc. Camb. Philos. Soc.* 66: 335–344, 1968

[Cow20] Alex Cowan. Conjecture: 100% of elliptic surfaces over $\mathbb{Q}$ have rank zero. *Preprint available at* https://arxiv.org/pdf/2009.08622.pdf, 2020.

[Des18] Julie Desjardins. Root number in non-isotrivial integer parameter families of elliptic curves. *Preprint available at* https://arxiv.org/pdf/1810.12787.pdf, 2018.

[Des19a] Julie Desjardins. On the density of rational points on rational elliptic surfaces. *Acta Arith.*, 189(2):109–146, 2019.

[Des19b] Julie Desjardins. On the variation of the root number in families of elliptic curves. *J. Lond. Math. Soc. (2)*, 99(2):295–331, 2019.

[DHP15]   Chantal David, Duc Khiem Huynh, and James Parks. One-level density of families of elliptic curves and the Ratios Conjecture. *Res. Number Theory*, 1:Paper No. 6, 37, 2015.

[Fer97]   Stéfane Fermigier. Une courbe elliptique définie sur **Q** de rang ≥ 22. *Acta Arith.*, 82(4):359–363, 1997.

[Gol79]   D. Goldfeld. Conjectures on elliptic curves over quadratic fields. *Number theory*, Carbondale 1979 (*Proc. Southern Illinois Conf., Southern Illinois Univ., Carbondale, Ill.*, 1979), pp. 108–118, *Lecture Notes in Math.*, 751, Springer, Berlin, 1979.

[Hel09]   Harald Helfgott. On the behaviour of root numbers in families of elliptic curves. *Preprint*, arXiv:math/0408141v3.

[Klo22]   Remke Kloosterman The average Mordell-Weil rank of elliptic surfaces over number fields. *Preprint available at* `https://arxiv.org/abs/2204.12102`, 2022.

[Kub09]   Gerald Kuba. On the distribution of reducible polynomials. *Math. Slovaca*, 59(3):349–356, 2009.

[Maz92]   Barry Mazur. The topology of rational points. *Experiment. Math.*, 1(1):35–45, 1992.

[Mes91]   Jean-François Mestre. Courbes elliptiques de rang ≥ 12 sur **Q**(t). *C. R. Acad. Sci. Paris Sér. I Math.*, 313(4):171–174, 1991.

[Mil06]   Steven J. Miller. Investigations of zeros near the central point of elliptic curve L-functions. *Experiment. Math.*, 15(3):257–279, 2006. With an appendix by Eduardo Dueñez.

[Ros02]   Michael Rosen *Number Theory in Function Fields*, volume 210 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 2002.

[RS01]   Karl Rubin and Alice Silverberg. Rank frequencies for quadratic twists of elliptic curves. *Experiment. Math.*, 10(4):559–569, 2001.

[SS10]   Matthias Schütt and Tetsuji Shioda. Elliptic surfaces. In *Algebraic geometry in East Asia—Seoul 2008*, volume 60 of *Adv. Stud. Pure Math.*, pages 51–160. Math. Soc. Japan, Tokyo, 2010.

[ST95]   C. L. Stewart and J. Top. On ranks of twists of elliptic curves and power-free values of binary forms. *J. Amer. Math. Soc.*, 8(4):943–973, 1995.

DIPARTIMENTO DI MATEMATICA, UNIVERSITÀ DEGLI STUDI DI MILA, VIA SALDINI 50, 20133 MILANO, ITALY
  Email address: `francesco.battistoni@unimi.it`

DIPARTIMENTO DI MATEMATICA, UNIVERSITÀ DI GENOVA, VIA DODECANESO 35, 16146 GENOVA, ITALY
  Email address: `bettin@dima.unige.it`

LABORATOIRE DE MATHÉMATIQUES DE BESANÇON, UNIVERSITÉ DE BOURGOGNE FRANCHE-COMTÉ, CNRS UMR 6623, 16, ROUTE DE RAY, 25030 BESANÇON CEDEX, FRANCE
  Email address: `christophe.delaunay@univ-fcomte.fr`