THE ELLIPTIC SIEVE

E. KOWALSKI

In a paper in progress ("The algebraic principle of the large sieve"), the author has developed a general abstract form of the large sieve inequality that covers both classical instances and the more recent "sieve for Frobenius" of [Ko1].[1] Looking for further applications of this general setting, the following case suggested itself (among others). Since it is of some independent interest, and quite simple, and since in fact it may be presented independently of the general development, we will present it here in a short note; the results will be incorporated in the paper already mentioned.

The sieve in question is performed on the Mordell-Weil group of rational points on an elliptic curve $E/\mathbf{Q}$; the application we derive concerns the number of prime divisors of the denominators of those rational points. This, in turn, is related to the analysis of the prime factorization of elements of so-called "elliptic divisibility sequences", and we find that "most" elements have many prime factors. This complements recent heuristics and results of Silverman, Everest, T. Ward, M. Ward and others concerning the paucity of primes and prime powers in such sequences.

Let $E/\mathbf{Q}$ be an elliptic curve given by a Weierstrass equation

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6, \quad \text{where } a_i \in \mathbf{Z}.$$

We assume that the rank r of E is positive, so there are infinitely many rational points. Let Λ be the set of primes ℓ of good reduction, and for $\ell \in \Lambda$, let $\rho_\ell : E(\mathbf{Q}) \to E(\mathbf{F}_\ell)$ be the reduction map.

The natural sets $X \subset E(\mathbf{Q})$ for sieving are the sets of rational points $x \in E(\mathbf{Q})$ with (canonical or naive) height $h(x) \leqslant T$ for some $T \geqslant 0$. To see the sieve potential, let $\Omega_\ell = \{0\}$, and notice that a rational point $x = (r, s) \in E(\mathbf{Q})$ (in affine coordinates, so $x \neq 0$) has reduction modulo $\ell \in \Lambda$ lying outside Ω_ℓ, if and only if ℓ does not appear in the denominator of the coordinates r and s of the point, which shows that integral points (in the affine model above) or S-integral points appear naturally as (subsets of) sifted sets in this context.

Here is the main result of this note. In this statement, we denote by $\omega_E(x)$ the number of primes occuring in the denominator of a rational point $x \neq 0$, without counting multiplicity, and by convention we put $\omega_E(0) = +\infty$. Then we have:

Proposition 1. *Let $E/\mathbf{Q}$ be an elliptic curve with rank $r \geqslant 1$. Then we have*

$$|\{x \in E(\mathbf{Q}) \mid h(x) \leqslant T\}| \sim c_E T^{r/2} \tag{1}$$

as $T \to +\infty$, for some constant $c_E > 0$, and moreover for any fixed real number κ with $0 < \kappa < 1$, we have

$$|\{x \in E(\mathbf{Q}) \mid h(x) \leqslant T \text{ and } \omega_E(x) < \kappa \log\log T\}| \ll T^{r/2}(\log\log T)^{-1},$$

for $T \geqslant 3$, where the implied constant depends only on E and κ.

Proof. Let $M \simeq \mathbf{Z}^r$ be a subgroup of $E(\mathbf{Q})$ such that

$$E(\mathbf{Q}) = M \oplus E(\mathbf{Q})_{tors},$$

and let $(x_1, \dots, x_r)$ be a fixed $\mathbf{Z}$-basis of M. Moreover, let M' be the group generated by $(x_2, \dots, x_r)$. We will in fact perform sieving only on "lines" directed by x_1.

Key words and phrases. Large sieve inequalities, elliptic divisibility sequences.

[1] A similar abstract framework was also developped independently by D. Zywina.

But first of all, since the canonical height is a positive definite quadratic form on $E(\mathbf{Q})$, the asymptotic formula (1) is clear: it amounts to nothing else but counting integral points in $M \otimes \mathbf{R} \simeq \mathbf{R}^r$ with norm $\sqrt{h(x)} \leqslant \sqrt{T}$, as many times as there are torsion points.

Moreover, we may (for convenience) measure the size of elements in $E(\mathbf{Q})$ by the squared L^∞-norm

$$\|x\|_\infty^2 = \max |a_i|^2, \quad \text{for } x = \sum a_i x_i + t \text{ with } t \in E(\mathbf{Q})_{tors},$$

i.e, we have $h(x) \asymp \|x\|_\infty^2$ for all $x \in M$, the implied constants depending only on E.

Now we claim the following:

Lemma 2. *For any fixed $\kappa \in]0,1[$, any fixed $x' \in M'$, any fixed torsion point $t \in E(\mathbf{Q})_{tors}$, we have*

$$|\{x \in t + x' \oplus \mathbf{Z}x_1 \mid \|x\|_\infty^2 \leqslant T \text{ and } \omega_E(x) < \kappa \log\log T\}| \ll \sqrt{T}(\log\log T)^{-1},$$

for $T \geqslant 3$, the implied constant depending only on E, κ and x_1, but not on x' or t.

Taking this for granted, we conclude immediately that

$$|\{x \in E(\mathbf{Q}) \mid h(x) \leqslant T \text{ and } \omega_E(x) < \kappa \log\log T\}| \ll T^{r/2}(\log\log T)^{-1},$$

by summing the inequality of the lemma over all $x' \in M'$ with $\|x'\|_\infty^2 \leqslant T$ and over all $t \in E(\mathbf{Q})_{tors}$, the number of which is $\ll T^{(r-1)/2}$, the implied constant depending only on E and the choice of basis of M.

Next we come to the proof of this lemma. Fix $x' \in M'$, $t \in E(\mathbf{Q})_{tors}$. The left-hand side of the lemma being zero unless $\|t + x'\|_\infty^2 \leqslant T$, we assume that this is the case. Denote

$$G = \mathbf{Z}x_1 \subset E(\mathbf{Q}), \qquad G_\ell = \rho_\ell(G) \subset E_\ell = \rho_\ell(E(\mathbf{Q}))$$
$$X = \{mx_1 \in G \mid \|t + x' + mx_1\|_\infty^2 = m^2 \leqslant T\};$$

we will "sieve" the set X using "reductions" modulo certain primes in Λ.

For any prime $\ell \in \Lambda$, the finite group G_ℓ is a quotient of $\mathbf{Z}x_1$ and is isomorphic to $\mathbf{Z}/\nu(\ell)\mathbf{Z}$ where $\nu(\ell)$ is the order of the reduction of x_1 modulo ℓ. Now we appeal to the following consequence of a result of Silverman ([Si1, Prop. 10]): all but finitely many primes p occur as the order $\nu(\ell) = p$ of x_1 for some prime ℓ of good reduction. For any $L \geqslant 2$, this enables us to sieve X using the finite set $\mathcal{L}$ of primes $\ell \in \Lambda$ such that $\nu(\ell) \leqslant L$ is a prime number $p \leqslant L$ (where, in case the same prime p occurs as values of $\nu(\ell)$ for two or more primes, we keep only one).

More precisely, we claim that the following large-sieve inequality

$$\sum_{\ell \in \mathcal{L}} \sideset{}{^*}\sum_{a \,(\mathrm{mod}\, \nu(\ell))} \Big| \sum_{|m| \leqslant \sqrt{T}} \alpha(m) e\Big(\frac{am}{\nu(\ell)}\Big)\Big|^2 \leqslant \Delta \sum_{|m| \leqslant \sqrt{T}} |\alpha(m)|^2, \tag{2}$$

holds for arbitrary complex numbers $\alpha(m)$ with

$$\Delta \leqslant 2\sqrt{T} + L^2$$

for $L \geqslant 2$, where the implied constant depends only on E (once x_1 is fixed, as it is throughout). Indeed, since $\nu(\ell)$ runs once over all but finitely many primes $p \leqslant L$, this follows by positivity from the "standard" large-sieve inequality (see e.g. [B], [IK, §7.5], [G], [Mo]):

$$\sum_{p \leqslant L} \sideset{}{^*}\sum_{a \,(\mathrm{mod}\, p)} \Big| \sum_{|m| \leqslant \sqrt{T}} \alpha(m) e\Big(\frac{am}{p}\Big)\Big|^2 \leqslant (2\sqrt{T} + L^2) \sum_{|m| \leqslant \sqrt{T}} |\alpha(m)|^2.$$

It then follows that

$$\sum_{x \in X} \Big(P(x, \mathcal{L}) - P(\mathcal{L})\Big)^2 \leqslant \Delta P(\mathcal{L}) \tag{3}$$

where $P(x,\mathcal{L})$ and $P(\mathcal{L})$ are defined by

$$P(x,\mathcal{L}) = \sum_{\substack{\ell\in\mathcal{L}\\ \rho_\ell(x)\in\Omega_\ell}} 1, \qquad P(\mathcal{L}) = \sum_{\ell\in\mathcal{L}} \frac{|\Omega_\ell|}{\nu(\ell)},$$

for any given choice of sets $\Omega_\ell \subset G_\ell$ for $\ell \in \Lambda$ (see e.g. [G, Lemma A]).

We let $\Omega_\ell = \{-\rho_\ell(t+x')\}$. By the remarks before the statement of the proposition, we have $\rho_\ell(mx_1) \in \Omega_\ell$ if and only if ℓ divides the denominator of the coordinates of $t + x' + mx_1$, and therefore for $x = mx_1 \in X$, we have

$$P(mx_1,\mathcal{L}) \leqslant \omega_E(t + x' + mx_1).$$

On the other hand, we have the lower bound

$$P(\mathcal{L}) = \sum_{\ell\in\mathcal{L}} \frac{1}{|G_\ell|} = \sum_{\substack{\ell\in\Lambda\\ \nu(\ell)\leqslant L}} \frac{1}{\nu(\ell)} \geqslant \sum_{p\leqslant L} \frac{1}{p} + O(1) = \log\log L + O(1)$$

for any $L \geqslant 3$, because, by Silverman's result, the values $\nu(\ell) \leqslant L$ range over all primes $\leqslant L$, with only finitely many exceptions (independently of L).

Hence there exists L_0 depending on E, x_1 and κ only, such that if $L \geqslant L_0$, we have

$$P(\mathcal{L}) \geqslant \frac{1+\kappa}{2}\log\log T.$$

Putting together these two inequalities, we see that if $L \geqslant L_0$, then for any $mx_1 \in X$ such that $t + x' + mx_1$ satisfies $\omega_E(t + x' + mx_1) < \kappa \log\log T$, we have

$$\Big(P(x,\mathcal{L}) - P(\mathcal{L})\Big)^2 \gg (\log\log T)^2,$$

the implied constant depending only on E, x_1 and κ. So it follows by positivity from (3) that

$$\begin{aligned}|\{x \in t + x' \oplus \mathbf{Z}x_1 \mid \|x\|_\infty^2 \leqslant T \text{ and } \omega_E(x) < \kappa\log\log T\}| &\ll \Delta(\log\log T)^{-1}\\ &\ll (\sqrt{T} + L^2)(\log\log T)^{-1}\end{aligned}$$

for any $L \geqslant L_0$. If $T^{1/2} \geqslant L_0$, we take $L = T^{1/2}$ and prove the inequality of the lemma directly, and otherwise we need only increase the resulting implied constant since L_0 depends only on E, x_1 and κ. □

Remark 3. It would be interesting to know whether there is some "regular" distribution for the function $\omega_E(x)$. Notice the similarity between the above discussion and the Hardy-Ramanujan results concerning the normal order of the number of prime divisors of an integer (see e.g. [HW, 22.11]), but note that since the denominators of rational points x are typically of size $\exp h(x)$, they should have around $\log\log\exp(h(x)) = \log(h(x))$ prime divisors in order to be "typical" integers.

However, we can also note that the prime divisors accounted for in the proof above are all $\leqslant T^{1/2} \simeq \sqrt{h(x)} \simeq \sqrt{\log n}$; it *is* typical behavior for an integer $n \leqslant T$ to have roughly $\log\log\log T$ prime divisors of this size (much more precise results of this type are due to Erdös and Kac, Erdös and Turán).

We can relate Proposition 1, or more precisely Lemma 2, to so-called *elliptic divisibility sequences*, a notion introduced by M. Ward and currently the subject of a number of investigations by Silverman, T. Ward, Everest, and others (see e.g. [Si2], [W], [EEW]).

Proposition 4. *Let* $(W_n)_{n\geqslant 0}$ *be an* unbounded *sequence of integers such that*

$$W_0 = 0, \quad W_1 = 1, \quad W_2W_3 \neq 0, \quad W_2 \mid W_4$$

$$W_{m+n}W_{m-n} = W_{m+1}W_{m-1}W_n^2 - W_{n+1}W_{n-1}W_m^2, \quad \textit{for } m \geqslant n \geqslant 1,$$

$$\begin{aligned}\Delta = W_4W_2^{15} - W_3^3W_2^{12} + 3W_4^2W_2^{10} - 20W_4W_3^3W_2^7\\ +4W_4^3W_2^5 + 16W_3^6W_2^4 + 8W_4^2W_3^3W_2^2 + W_4^4 \neq 0.\end{aligned}$$

Then for any κ such that $0 < \kappa < 1$, we have

$$|\{n \leqslant N \mid \omega(W_n) < \kappa \log\log N\}| \ll \frac{N}{\log\log N},$$

for $N \geqslant 3$, the implied constant depending only on (W_n) and κ.

Proof. This depends on the relation between elliptic divisibility sequences and pairs (E, x_0) of an elliptic curve $E/\mathbf{Q}$ and a point $x_1 \in E(\mathbf{Q})$. Precisely (see e.g. [EEW, §2]) there exists such a pair (E, x_1) with x_1 of infinite order such that if (a_n), (b_n), (d_n) are the (unique) sequences of integers with $d_n \geqslant 1$, $(a_n, d_n) = (b_n, d_n) = 1$ and

$$nx_1 = \Big(\frac{a_n}{d_n^2}, \frac{b_n}{d_n^3}\Big),$$

then we have

$$d_n \mid W_n \text{ for } n \geqslant 1$$

(without the condition $\Delta = 0$, this is still true provided *singular* elliptic curves are permitted; the condition that (W_n) be unbounded implies that x_0 is of infinite order).

Now the d_n are precisely the denominators of the coordinates of the points in $\mathbf{Z}x_1$, and we have therefore

$$\omega(W_n) \geqslant \omega(d_n) = \omega_E(nx_1).$$

Hence Lemma 1 gives the desired result. □

The "simplest" example is the sequence (W_n) given by

$$W_0 = 0, \quad W_1 = 1, \quad W_2 = 1, \quad W_3 = -1, \quad W_4 = 1,$$

$$W_n = \frac{W_{n-1}W_{n-3} + W_{n-2}^2}{W_{n-4}}, \quad \text{for } n \geqslant 4$$

(sequence `A006769` in the Online Encyclopedia of Integer Sequences), which corresponds to case of $E : y^2 + y = x^3 - x$ and $x_0 = (0, 0)$.

Finally, it will be noticed that the same reasoning and similar results hold for elements of non-degenerate divisibility sequences (u_n) defined by linear recurrence relations of order 2, e.g., $u_n = a^n - 1$ where $a \geqslant 2$ is an integer. (The analogue of Silverman's theorem here is a result of Schinzel, and the rest is easy).

References

[B] E. Bombieri: *Le grand crible dans la théorie analytique des nombres*, Astérisque 18, S.M.F (1974).

[EEW] M. Einsiedler, G. Everest and T. Ward: *Primes in elliptic divisibility sequences*, LMS J. Comput. Math. 4 (2001), 1–13.

[G] P.X. Gallagher: *The large sieve and probabilistic Galois theory*, in Proc. Sympos. Pure Math., Vol. XXIV, Amer. Math. Soc. (1973), 91–101.

[HW] G.H. Hardy and E.M. Wright: *An introduction to the theory of numbers*, Fifth Edition, Oxford 1979.

[IK] H. Iwaniec and E. Kowalski: *Analytic Number Theory*, A.M.S Colloquium Publ. 53, 2004.

[Ko1] E. Kowalski: *The large sieve, monodromy and zeta functions of curves*, J. reine angew. Math, to appear, `arXiv:math.NT/0503714`

[Mo] H.L. Montgomery: *The analytic principle of the large sieve*, Bull. A.M.S 84 (1978), 547–567.

[Si1] J. Silverman: *Wieferich's criterion and the abc-Conjecture*, J. of Number Theory 30 (1988), 226–237.

[Si2] J. Silverman: *p-adic properties of division polynomials and elliptic divisibility sequences*, Math. Ann. 332 (2005), 443–471.

[W] M. Ward: *Memoir on elliptic divisibility sequences*, Amer. J. Math. 70 (1948), 31–74.

Université Bordeaux I - IMB, 351, cours de la Libération, 33405 Talence Cedex, France
E-mail address: `emmanuel.kowalski@math.u-bordeaux1.fr`