Canad. Math. Bull. Vol. **57** (1), 2014 pp. 105–112
http://dx.doi.org/10.4153/CMB-2012-037-4

On the Counting Function of Elliptic Carmichael Numbers

Florian Luca and Igor E. Shparlinski

Abstract. We give an upper bound for the number of elliptic Carmichael numbers $n \le x$ that were recently introduced by J. H. Silverman in the case of an elliptic curve without complex multiplication (non CM). We also discuss several possible further improvements.

1 Introduction

Let E be an elliptic curve over the field of rational numbers $\mathbb{Q}$ given by an *affine Weierstraß equation*:

$$E : Y^2 = X^3 + aX + b.$$

In particular, it has a nonzero discriminant $\Delta = 4a^3 + 27b^2$. We refer to [7] for a background on elliptic curves. For a prime p, we define a_p by $\#E(\mathbb{F}_p) = p + 1 - a_p$, where $E(\mathbb{F}_p)$ in the set of $\mathbb{F}_p$-rational points on the reduction of E modulo p including the point at infinity O_p. We also recall that if $p \nmid \Delta$, then $E(\mathbb{F}_p)$ has a structure of an Abelian group (see [7, Chapter III, Section 2]).

Since $a_p = O(p^{1/2})$ by the Hasse bound (see, for example, [7, Chapter V, Theorem 1.1]), for $\Re s > 3/2$ we can define the L-function

$$L(s) = \prod_{p \mid \Delta} (1 - a_p p^{-s})^{-1} \prod_{p \nmid \Delta} (1 - a_p p^{-s} + p^{1-2s})^{-1},$$

which we expand to the power series

$$L(s) = \sum_{n=1}^{\infty} \frac{a_n}{n^s}$$

(see, for example, [7, Chapter V, Exercise 8.19]).

Slightly relaxing the definition given in [8] and thus expanding the class of numbers we consider, we say that a positive integer n is an *E-Carmichael number* if

- it is not a prime power;
- $gcd(n, \Delta) = 1$;

Received by the editors June 15, 2012; revised August 21, 2012.
Published electronically November 13, 2012.
During the preparation of this paper, F. L. was supported in part by Project PAPIIT IN104512 and a Marcos Moshinsky fellowship, and I. S. was supported by ARC Grant DP1092835 (Australia) and NRF Grant CRP2-2007-03 (Singapore).
AMS subject classification: **11Y11**, 11N36.
Keywords: elliptic Carmichael numbers, applications of sieve methods.

- for any point $P \in E(\mathbb{F}_p)$ we have

$$(n+1-a_n)P = O_p, \tag{1.1}$$

where both the equation and the group law are considered over $\mathbb{F}_p$.

In this paper, we address only the instance of non CM curves E, which are those curves whose endomorphism ring over the field of complex numbers consists of the ring of integers; that is, their only endomorphisms are the maps n_E, which, for a fixed integer n, send P to nP for all $P \in E(\mathbb{C})$. We show that the sequence of E-Carmichael numbers is of asymptotic density zero.

2 Notation

We recall that the notations $U = O(V)$, $U \ll V$ and $V \gg U$ are all equivalent to the statement that the inequality $|U| \le cV$ holds with some constant $c > 0$. Throughout the paper, any implied constants in the symbols O, $\ll$, and $\gg$ may occasionally depend, where obvious, on the curve E, and are absolute otherwise.

We write $\log_1 x = \max\{1, \log x\}$. For an integer $k \ge 2$, we write $\log_k x$ for the iteratively defined function given by $\log_k x = \log_1(\log_{k-1} x)$. When $k = 1$ we omit the subscript and thus understand that all natural logarithms that appear exceed 1.

3 Main Result

For a real $x \ge 1$, let $N_E(x)$ be the number of E-Carmichael numbers $n \le x$.

Theorem 3.1 *Let E be a non CM curve. For a sufficiently large x*

$$N_E(x) \ll \frac{x \log_3 x}{\log_2 x}.$$

4 Preparations

We need a version of the following result of David and Wu [4, Theorem 2.3(i)], which improves and generalizes several previous bounds (see [2, 3]). For integers a and $t \ge 1$ let

$$\pi_E(x; a, t) = \#\big\{ p \le x : \#E(\mathbb{F}_p) \equiv a \pmod t \big\}.$$

Let $\varphi(k)$ denote the Euler function of the positive integer k. Then David and Wu [4, Proposition 2.1] show that if E is a non CM curve, the estimate

$$\pi_E(x; a, t) \ll \frac{\pi(x)}{\varphi(t)} + x \exp\big(-At^{-2}\sqrt{\log x}\big). \tag{4.1}$$

holds uniformly for $\log x \gg t^{12} \log t$, where A is an absolute constant and the implied constant depends only on E.

https://doi.org/10.4153/CMB-2012-037-4 Published online by Cambridge University Press

We prove that a slightly weaker result holds for the counting function of the primes p for which p and a_p satisfy a certain type of linear relation modulo a positive integer t. The result is uniform in the coefficients of the linear relation. More precisely, let U and V be fixed integers and let

$$\pi_{E,U,V}(x;t) = \#\big\{\, p \le x : Up + 1 - Va_p \equiv 0 \pmod{t}\big\},$$

respectively. We have the following result. Let $\tau(t)$ denote the number of divisors of the positive integer t.

Lemma 4.1 *Let E be a non CM curve. The estimate*

$$\pi_{E,U,V}(x;t) \ll \frac{\tau(t)\pi(x)(\log\log t)^{\kappa}}{t} + x\exp\big(-At^{-2}\sqrt{\log x}\big)$$

holds uniformly for integers U and V and for $\log x \gg t^{12}\log t$, where the implied constants depend only on the elliptic curve E. Here A and κ are positive absolute constants.

Proof We follow the notation and arguments from [4, Section 2]. Let $\mathbb{L}_t$ be the field extension of $\mathbb{Q}$ obtained by adjoining to $\mathbb{Q}$ the coordinates of the t-torsion points of E and let $G_t = \mathrm{Gal}(\mathbb{L}_t/\mathbb{Q})$. Since $E[t](\overline{\mathbb{Q}}) \cong \mathbb{Z}/t\mathbb{Z} \times \mathbb{Z}/t\mathbb{Z}$, by fixing a basis for the t-torsion one gets an injective map $\rho_t\colon\ G_t \mapsto \mathrm{GL}_2(\mathbb{Z}/t\mathbb{Z})$, so we identify G_t with some subgroup of $\mathrm{GL}_2(\mathbb{Z}/t\mathbb{Z})$ via the map ρ_t. For unramified primes p, let σ_p be the Artin symbol of $\mathbb{L}_t/\mathbb{Q}$. Then $\rho_t(\sigma_p)$ can be identified with a conjugacy class of matrices in $\mathrm{GL}_2(\mathbb{Z}/t\mathbb{Z})$. Furthermore, under such identification, for the trace and determinant of $\rho(\sigma_p)$ we have $\mathrm{tr}(\rho_t(\sigma_p)) \equiv a_p \pmod{t}$ and $\det(\rho_t(\sigma_p)) \equiv p \pmod{t}$, respectively. Thus, in order to count such primes p, we need to count matrices $g \in G_t$ such that

$$U\det(g) + 1 - V\,\mathrm{tr}(g) \equiv 0 \pmod{t}.$$

We write $C_{U,V}(t)$ for the set of such $g \in G_t$. Let M_E be a positive integer depending on E such that if $(t, M_E) = 1$, then $G_t = \mathrm{GL}_2(\mathbb{Z}/t\mathbb{Z})$. The existence of M_E has been proved by Serre [6]. Write $t = dm$, where $(d, M_E) = 1$ and m consists only of primes dividing M_E. Then the argument of David and Wu [4] based on Chebotarev's Density Theorem shows that

$$\pi_{E,A,B}(x;t) = \frac{\#C_{U,V}(m)}{\#G(m)}\Big(\prod_{\ell^k \| d}\frac{\#C_{U,V}(\ell^k)}{\#\,\mathrm{GL}_2(\mathbb{Z}/\ell^k\mathbb{Z})}\Big)\,\mathrm{Li}(x) + O\Big(x\exp\big(-At^{-2}\sqrt{\log x}\big)\Big), \tag{4.2}$$

provided that $\log x \gg t^{12}\log t$. David and Wu [4] carefully analyze the quotients $\#C_{U,V}(m)/\#G(m)$ and $\#C_{U,V}(\ell^k)|/\#\,\mathrm{GL}_2(\mathbb{Z}/\ell^k\mathbb{Z})$ when $U = V = 1$. While there is nothing in principle to stop us from performing the same analysis, we choose to only give upper bounds on the above quantities, which are both easy to prove and sufficient for our present purpose.

https://doi.org/10.4153/CMB-2012-037-4 Published online by Cambridge University Press

Assume that $\ell \nmid M_E$. We write $g = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$. Then we need to count the number of (a, b, c, d) in $\mathbb{Z}/\ell^k\mathbb{Z}$ such that

$$U(ad - bc) + 1 - V(a + d) \equiv 0 \pmod{\ell^k}.$$

Rewrite the above congruence as

$$(Ua - V)d \equiv -1 + Ubc + Va \pmod{\ell^k}.$$

Consider first the case when $Ua \equiv V \pmod{\ell^k}$. Then also

$$Va \equiv 1 - Ubc \pmod{\ell^k}.$$

In this case, either $\ell \nmid U$ or $\ell \nmid V$. From the above congruences, we conclude that a is uniquely determined in terms of b and c, and d is arbitrary, so the number of such g is at most ℓ^{3k}.

Next, let $i \in \{0, 1, \ldots, k-1\}$ be such that $Ua - V \equiv 0 \pmod{\ell^i}$, but $Ua - V \not\equiv 0 \pmod{\ell^{i+1}}$. Again, as in the previous argument, we must have $Va + Ubc - 1 \equiv 0 \pmod{\ell^i}$, otherwise there is no such g. Since one of U or V is not a multiple of ℓ, we conclude that a is unique modulo ℓ^i when b and c are fixed, so the number of lifts of a modulo ℓ^k is at most ℓ^{k-i}. Further, we have

$$d(Ua - V)/\ell^i \equiv (-1 + Ubc + Va)/\ell^i \pmod{\ell^{k-i}},$$

so d is uniquely determined modulo ℓ^{k-i}, therefore the number of lifts of d modulo ℓ^k is at most ℓ^i. Since b and c can take at most ℓ^k values each, it follows that the number of possibilities for (a, b, c, d) is at most $\ell^{k-i} \times \ell^k \times \ell^k \times \ell^i = \ell^{3k}$. Giving to i the values $0, 1, \ldots, k-1$, and summing up the above bounds, we conclude that

$$\#C_{U,V}(\ell^k) \le (k+1)\ell^{4k}.$$

Thus,

$$\frac{\#C_{U,V}(\ell^k)}{\#\,\mathrm{GL}_2(\mathbb{Z}/\ell^k\mathbb{Z})} \le \frac{(k+1)\ell^{3k}}{\ell^{4k}(1 + O(1/\ell))} \le \frac{\tau(\ell^k)}{\ell^k}\left(1 + \frac{1}{\ell}\right)^{\kappa}$$

for some absolute constant κ. Multiplying the above inequalities for all $\ell^k \| d$, we get that

$$\prod_{\ell^k \| d} \frac{\#C_{U,V}(\ell^k)}{\#\,\mathrm{GL}_2(\mathbb{Z}/\ell^k\mathbb{Z})} \le \prod_{\ell^k \| d} \frac{\tau(\ell^k)}{\ell^k}\left(1 + \frac{1}{\ell}\right)^{\kappa} \le \frac{\tau(d)}{d}\left(\frac{\sigma(d)}{d}\right)^{\kappa} \ll \frac{\tau(d)}{d}(\log\log d)^{\kappa}, \tag{4.3}$$

where $\sigma(d)$ is the sum of the divisors of d and we have used the well-known bound $\sigma(d)/d \ll \log\log d$. A similar analysis can be performed to show that

$$\frac{\#C_{U,V}(m)}{\#G(m)} \ll \frac{1}{m}. \tag{4.4}$$

Putting (4.3) and (4.4) into (4.2), we get the desired inequality on $\pi_{E,U,V}(x; t)$. ∎

https://doi.org/10.4153/CMB-2012-037-4 Published online by Cambridge University Press

5 Proof of Theorem 3.1

We write x for a large positive real number. We also write w, y, and z for parameters depending on x that tend to infinity with x and which is to be made more precise later.

Let t_p be the exponent of the group $E(\mathbb{F}_p)$, that is, the largest possible order of any point $P \in E(\mathbb{F}_p)$.

We see from (1.1) that for any E-Carmichael number n we have

$$t_p \mid n + 1 - a_n \tag{5.1}$$

for all primes $p \mid n$.

Now fix some $z > y > 1$ and remove $n \le x$ without a prime divisor in $[y, z]$. Let $\mathcal{E}_1(x)$ be the set of such n. By the Brun sieve ([9, Section I.4.2]) and Mertens' formula ([9, Section I.1.6]), we have

$$\#\mathcal{E}_1(x) \ll x \prod_{y \le p \le z} \Big(1 - \frac{1}{p}\Big) \ll x\Big(\frac{\log y}{\log z}\Big). \tag{5.2}$$

Then remove all $n \le x$ such that $p^2 \mid n$ for some $p \ge y$. Let $\mathcal{E}_2(x)$ be the set of such n. Fixing p, the number of $n \le x$ that are divisible by p^2 is at most x/p^2. Hence,

$$\#\mathcal{E}_2(x) \le \sum_{y \le p} \frac{x}{p^2} = O\Big(\frac{x}{y}\Big). \tag{5.3}$$

Let $P(n)$ be the largest prime factor of n. We remove $n \le x$ such that $P(n) \le w$, where

$$w = \exp\Big(\frac{\log x \log_4 x}{2 \log_3 x}\Big).$$

Put $\mathcal{E}_3(x)$ for the set of such n. It is well known that

$$\#\mathcal{E}_3(x) = \frac{x}{\exp((1 + o(1))u \log u)},$$

as $x \to \infty$, where

$$u = \frac{\log x}{\log w} = \frac{2 \log_3 x}{\log_4 x}$$

(see, for example, [1, Corollary, p. 15]). Since $u \log u = (2 + o(1)) \log_3 x$ as $x \to \infty$, we derive

$$\#\mathcal{E}_3(x) = \frac{x}{(\log_2 x)^{2+o(1)}} = O\Big(\frac{x}{\log_2 x}\Big). \tag{5.4}$$

Assume that $w > 2z$. Then any remaining integer $n \le x$ can be written under the form $n = pPm$, where $p \in [y, z]$, $P = P(n) > w$ and pP is coprime to m. Since the coefficient a_n is a multiplicative function of n, we have $a_n = a_m a_p a_P$. Then we see from (5.1) that

$$t_p \mid mPp + 1 - a_m a_p a_P. \tag{5.5}$$

https://doi.org/10.4153/CMB-2012-037-4 Published online by Cambridge University Press

Note that $t_p \gg p^{1/2}$ (see [5] for a slightly more precise result). We fix $p \in [y, z]$ and m and count the number of choices for $P \le x/mp$. Put $U = mp$ and $V = a_m a_p$. Relation (5.5) implies

$$UP + 1 - Va_P \equiv 0 \pmod{t_p}.$$

By Lemma 4.1, we derive that number of such $P \le x/(mp)$ is of order at most

$$\frac{\tau(t_p)\pi(x/mp)(\log\log t_p)^\kappa}{t_p} + \frac{x}{mp}\exp\bigl(-At_p^{-2}\sqrt{\log(x/mp)}\bigr) \ll \frac{x(\log\log p)^\kappa}{mpt_p\log(x/mp)} + \frac{x}{mp}\exp\bigl(-At_p^{-2}\sqrt{\log(x/mp)}\bigr), \tag{5.6}$$

provided that

$$t_p \log t_p \le \bigl(\log(x/mp)\bigr)^{1/12}. \tag{5.7}$$

Since $t_p \le 2z$, $x/mp \ge P \ge w$, and

$$\log(x/mp) \ge \log w \ge \frac{\log x \log_3 x}{\log_2 x},$$

it follows that inequality (5.7) holds if we choose $z \le (\log x)^{1/13}$ and x is sufficiently large. For such values of x and z, the second term in the estimate (5.6) is

$$\frac{x}{mp}\exp\bigl(-At_p^{-2}\sqrt{\log(x/mp)}\bigr) \le \frac{x}{mp}\exp\Bigl(-A(\log x)^{11/26}\Bigl(\frac{\log_3 x}{\log_2 x}\Bigr)^{1/2}\Bigr)$$

and is negligible compared with the first. So, the number of such primes $P \le x/(mp)$ is of order at most

$$\frac{\tau(t_p)x(\log\log p)^\kappa}{mpt_p\log(x/mp)} \ll \frac{\tau(t_p)x(\log_2 z)^\kappa}{mpt_p\log(x/mp)}.$$

Since $x/(mp) > P > w$, $t_p \gg p^{1/2}$, we get that the above estimate is of order at most

$$\frac{x\tau(t_p)(\log_3 x)(\log_2 z)^\kappa}{mp^{3/2}\log x\log_4 x}.$$

Now we sum up the above inequality over all $p \in [y, z]$ and $m \ge x$, getting a bound of shape

$$\frac{x\log_3 x(\log_2 z)^\kappa}{\log x\log_4 x}\sum_{y\le p\le z}\sum_{m\le x}\frac{\tau(t_p)}{mp^{3/2}} \ll \frac{x\log_3 x(\log_2 z)^\kappa}{y^{1/2+o(1)}\log_4 x},$$

as $x \to \infty$. Thus, we get that

$$\#\mathcal{E}_4(x) \le \frac{x\log_3 x(\log_2 z)^\kappa}{y^{1/2+o(1)}\log_4 x} \tag{5.8}$$

https://doi.org/10.4153/CMB-2012-037-4 Published online by Cambridge University Press

as $x \to \infty$. From the estimates (5.2), (5.3), (5.4), and (5.8), we conclude that

$$N_E(x) \ll x\Big(\frac{\log y}{\log z} + \frac{1}{y} + \frac{1}{\log_2 x} + \frac{\log_3 x(\log_2 z)^{\kappa}}{y^{1/2+o(1)}\log_4 x}\Big).$$

Since $z \le (\log x)^{1/13}$, the third term is dominated by the first, and the second term is dominated by the fourth. Thus,

$$N_E(x) \ll x\Big(\frac{\log y}{\log z} + \frac{\log_3 x(\log_2 z)^{\kappa}}{y^{1/2+o(1)}\log_4 x}\Big).$$

We now put $\varepsilon(x)$ for the function that is $o(1)$ appearing above, we choose

$$z = (\log x)^{1/14}, \quad y^{1/2+\varepsilon(x)}\log y = \frac{(\log_2 x)(\log_3 x)^{\kappa+1}}{\log_3 x},$$

and we derive the desired result.

6 Comments

We recall that under the Generalized Riemann Hypothesis, David and Wu [4, Theorem 2.3(iii)] show that one has the estimate

$$\pi_E(x;a,t) \ll \frac{\pi(x)}{\varphi(t)}$$

uniformly for $t \ll x^{1/8}/\log x$, instead of that of (4.1), and their argument can be extended similarly to Lemma 4.1 to cover the instance of $\pi_{E,U,V}(x;t)$. Using these bounds in our argument, one can easily obtain a conditional improvement of Theorem 3.1. It is also possible that for CM curves one can also obtain similar results. However, in order to get substantially better bounds, our argument, which treats the elements the set $\#\mathcal{E}_1(x)$ trivially and relies on the bound (5.2), ought to be augmented with some new ideas.

Another approach to a possible improvement of Theorem 3.1 is via a more efficient treatment of elements of the set $\mathcal{E}_4(x)$. In turn, this leads to a question of obtaining nontrivial upper bounds on the cardinality of the set

$$\{n \le x : a_n \equiv a \pmod{p}\}$$

for a prime p and an integer a (only the case $a = 1$ is relevant to our applications). Obtaining such bounds is certainly of independent interest.

Acknowledgments The authors would like to thank Alina Carmen Cojocaru for useful discussions and the anonymous referee for comments that improved the quality of the paper.

References

[1] E. R. Cranfield, P. Erdős, and C. Pomerance, *On a problem of Oppenheim concerning "factorisatio numerorum"*. J. Number Theory **17**(1983), no. 1, 1–28. http://dx.doi.org/10.1016/0022-314X(83)90002-1

[2] A. C. Cojocaru, É. Fouvry, and M. R. Murty, *The square sieve and the Lang–Trotter conjecture.* Canad. J. Math. **57**(2005), no. 6, 1155–1177. http://dx.doi.org/10.4153/CJM-2005-045-7

[3] A. C. Cojocaru, F. Luca, and I. E. Shparlinski, *Pseudoprime reductions of elliptic curves.* Math. Proc. Cambridge Philos. Soc. **146**(2009), no. 3, 513–522. http://dx.doi.org/10.1017/S0305004108001758

[4] C. David and J. Wu, *Pseudoprime reductions of elliptic curves.* Canad. J. Math. **64**(2012), no. 1, 81–101. http://dx.doi.org/10.4153/CJM-2011-044-x

[5] R. Schoof, *The exponents of the group of points on the reduction of an elliptic curve.* In: Arithmetic algebraic geometry (Texel, 1989), Progr. Math., 89, Birkhäuser Boston, Boston, MA, 1991, pp. 325–335.

[6] J.-P. Serre, *Propriétés galoisiennes des points d'ordre fini des courbes elliptiques.* Invent. Math. **15**(1972), no. 4, 259–331. http://dx.doi.org/10.1007/BF01405086

[7] J. H. Silverman, *Advanced topics in the arithmetic of elliptic curves.* Graduate Texts in Mathematics, 151, Springer-Verlag, Berlin, 1995.

[8] J. H. Silverman, *Elliptic Carmichael numbers and elliptic Korselt criteria.* arxiv:1108.3830.

[9] G. Tenenbaum, *Introduction to analytic and probabilistic number theory.* Cambridge Studies in Mathematics, 46, Cambridge University Press, Cambridge, 1995.

Centro de Ciencias Matemáticas, Universidad Nacional Autonoma de México, C.P. 58089, Morelia, Michoacán, México
e-mail: fluca@matmor.unam.mx

Department of Computing, Macquarie University, Sydney, NSW 2109, Australia
e-mail: igor.shparlinski@mq.edu.au