PROCEEDINGS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 143, Number 4, April 2015, Pages 1441–1448
S 0002-9939(2014)12345-8
Article electronically published on December 1, 2014

ON THE PRODUCT OF SMALL ELKIES PRIMES

IGOR E. SHPARLINSKI

(Communicated by Matthew A. Papanikolas)

ABSTRACT. Given an elliptic curve E over a finite field $\mathbb{F}_q$ of q elements, we say that an odd prime $\ell \nmid q$ is an Elkies prime for E if $t_E^2 - 4q$ is a quadratic residue modulo ℓ, where $t_E = q + 1 - \#E(\mathbb{F}_q)$ and $\#E(\mathbb{F}_q)$ is the number of $\mathbb{F}_q$-rational points on E. The Elkies primes are used in the presently most efficient algorithm to compute $\#E(\mathbb{F}_q)$. In particular, the quantity $L_q(E)$ defined as the smallest L such that the product of all Elkies primes for E up to L exceeds $4q^{1/2}$ is a crucial parameter of this algorithm. We show that there are infinitely many pairs (p, E) of primes p and curves E over $\mathbb{F}_p$ with $L_p(E) \geq c \log p \log\log\log p$ for some absolute constant $c > 0$, while a naive heuristic estimate suggests that $L_p(E) \sim \log p$. This complements recent upper bounds on $L_q(E)$ proposed by Galbraith and Satoh in 2002, conditional under the Generalised Riemann Hypothesis, and by Shparlinski and Sutherland in 2011, unconditional for almost all pairs (p, E).

1. INTRODUCTION

For an elliptic curve E over a finite field $\mathbb{F}_q$ of q elements we denote by $\#E(\mathbb{F}_q)$ the number of $\mathbb{F}_q$-rational points on E and define the *trace of Frobenius* $t_E = q + 1 - \#E(\mathbb{F}_q)$; we refer to [1, 13] for a background on elliptic curves.

We start with recalling that the first polynomial-time algorithm to compute $\#E(\mathbb{F}_q)$ is due to Schoof [11]. For a sufficiently large set of small primes ℓ, Schoof [11] determines $t_E \pmod{\ell}$ by computing the action of Frobenius on the ℓ-torsion subgroup $E[\ell] \cong \mathbb{Z}/\ell\mathbb{Z} \times \mathbb{Z}/\ell\mathbb{Z}$ and then determines the unique integer t_E that satisfies the Hasse bound $|t_E| \leq 2q^{1/2}$ via the Chinese remainder theorem. Elkies [5] has observed that when $t_E^2 - 4q$ is a quadratic residue modulo ℓ, one can instead work in a cyclic subgroup of $E[\ell]$, which speeds up the computation considerably. One can also obtain partial information at other primes ℓ, but this has no impact on the asymptotic performance of the algorithm.

We say that an odd prime $\ell \nmid q$ is an *Elkies prime* for E if $t_E^2 - 4q$ is a quadratic residue modulo ℓ; otherwise $\ell \nmid q$ is called an *Atkin prime*.

These primes play a key role in the *Schoof-Elkies-Atkin (SEA) algorithm*, see [1, Sections 17.2.2 and 17.2.5], and their distribution affects the performance of this algorithm in a rather dramatic way. Thus, for an elliptic curve E over $\mathbb{F}_q$, we define $N_a(E; L)$ and $N_e(E; L)$ as the numbers of Atkin and Elkies primes $\ell \in [1, L]$, respectively. Obviously,

$$N_a(E; L) + N_e(E; L) = \pi(L) + O(1),$$

Received by the editors January 9, 2013 and, in revised form, August 27, 2013.
2010 *Mathematics Subject Classification.* Primary 11G07, 11L40, 11Y16, 14G50.
Key words and phrases. Elliptic curves, Elkies primes, character sums.

where, as usual, $\pi(L)$ denotes the number of primes $\ell < L$. Furthermore, for any elliptic curve over a finite field, one expects about the same number of Atkin and Elkies primes $\ell < L$ as $L \to \infty$. That is, a naive heuristic argument suggests that

$$N_a(E; L) \sim N_e(E; L) \sim \frac{1}{2}\pi(L), \tag{1}$$

as $L \to \infty$.

It has been noted by Galbraith and Satoh [10, Appendix A], that under the Generalised Riemann Hypothesis (GRH), using the bound on sums of quadratic characters over primes, one can show that (1) holds for $L \geq (\log q)^{2+\varepsilon}$ for any fixed $\varepsilon > 0$ and a sufficiently large q.

The unconditional results are much weaker and essentially rely on our knowledge of the distribution of primes in arithmetic progressions; see [6, Section 5.9] or [9, Chapters 4 and 11]. However, for almost all pairs (p, E) of primes p and elliptic curves E over $\mathbb{F}_p$, Shparlinski and Sutherland [12] have established the asymtotic formula (1) for $L \geq (\log p)^{\varepsilon}$ for any fixed $\varepsilon > 0$, that is, starting from much smaller values of L than those implied by the GRH. In particular, let $\mathcal{L}_E(p)$ be the set of all Elkies primes for an elliptic curve E over $\mathbb{F}_p$. We see that the prime number theorem and the result of [12] implies that for some function $L(p) \sim \log p$ for almost all pairs (p, E) we have

$$\prod_{\substack{\ell \in \mathcal{L}_E(p)\\ 3 \leq \ell \leq L(p)}} \ell > 4p^{1/2}. \tag{2}$$

Note that this condition is crucial to the performance of the SEA point counting algorithm, see [1, Sections 17.2.2 and 17.2.5].

Here we show that this "almost all" result cannot be extended to all primes and curves even for a slightly larger values of $L(p)$. More precisely, we show that there is an absolute constant $c > 0$ such that for any function $L(p) \leq c \log p \log\log\log p$ the inequality (2) fails in a very strong sense for infinitely many pairs (p, E).

Theorem 1. *There is a constant $c > 0$ such that for infinitely many pairs (p, E) of primes p and curves E over $\mathbb{F}_p$, and $L \leq c \log p \log\log\log p$ we have*

$$\prod_{\substack{\ell \in \mathcal{L}_E(p)\\ 3 \leq \ell \leq L}} \ell = p^{o(1)}.$$

We note that Galbraith and Satoh [10, Appendix A] have conjectured and actually presented some arguments supporting a result of this kind. Moreover, under both the GRH and the conjecture that every positive integer $n \equiv 1 \pmod 4$ can be represented as $n = 4p - t^2$, the argument of Galbraith and Satoh [10, Appendix A] can be made rigorous, and in fact under these assumptions it allows one to replace $\log p \log\log\log p$ with $\log p \log\log p$ in Theorem 1. Unfortunately, the required representation $n = 4p - t^2$ is presently known to exist only for almost all n (see [2,7]), which is not enough to complete the argument (even under the GRH).

2. Preparations

We recall the notations $U = O(V)$, $V = \Omega(U)$, $U \ll V$ and $V \gg U$, which are all equivalent to the statement that the inequality $|U| \leq c\,V$ holds asymptotically, with some constant $c > 0$.

We always assume that ℓ and p run through the prime values.

For integers a and $m \ge 2$, we use (a/m) to denote a Jacobi symbol of a modulo m, see [6, Section 3.5]. We also use $\tau(k)$ and $\mu(k)$ to denote the number of positive integer divisors and the Möbius function of $k \ge 1$. It is easy to see that for a square-free k we have

$$\tau(k) = 2^{\omega(k)},$$

where $\omega(k)$ is the number of prime divisors of k.

Our main tools are bounds of multiplicative character sums.

The following estimate is a slight generalisation of [8, Lemma 2.2] and is also given in [12].

Lemma 2. *For any integers a and $T \ge 1$ and a product $m = \ell_1 \ldots \ell_s$ of $s \ge 0$ distinct odd primes $\ell_1, \ldots, \ell_s$ with $\gcd(a,m) = 1$ we have*

$$\sum_{|t|\le T} \left(\frac{t^2-a}{m}\right) \ll T/m + C^s m^{1/2} \log m,$$

for some absolute constant $C \ge 1$.

We also need a slight extension of [6, Corollary 12.14]. In fact, we present it in much wider generality and strength than is needed for our purpose. First we note that for a square-free integer m and any integers u and v, we have

$$\gcd((u-v)^2, m) = \gcd(u-v, m). \tag{3}$$

Hence, in the case of quadratic polynomials, the bound of [6, Theorem 12.10] implies the following result.

Lemma 3. *Assume that a square-free odd integer $m \ge 3$ and an arbitrary integer $N \ge 1$ are such that all prime factors of m are at most $N^{1/9}$. Then for any two integers u, v we have*

$$\left|\sum_{n=1}^{N} \left(\frac{(n-u)(n-v)}{m}\right)\right| \le 4N \left(\gcd(u-v,m) m^{-1} \tau(m)^{r^2+2r}\right)^{1/(r2^r)},$$

where r is any positive integer with $N^r > m^3$.

Proof. As in the proof of [6, Corollary 12.14], we note that there is a factorisation

$$m = m_1 \ldots m_r$$

with $m_j \le N^{4/9}$, $j = 1, \ldots, r$. In particular, by [6, Theorem 12.10], recalling (3), we see that for any $j = 1, \ldots, r$ we have

$$\left|\sum_{n=1}^{N} \left(\frac{(n-u)(n-v)}{m}\right)\right| \le 4N \left(\gcd(u-v,m_j) m_j^{-1} \tau(m_j)^{r^2+2r}\right)^{1/2^r}.$$

Since m is square-free, we see that $m_1, \ldots, m_r$ are relatively prime. Using the multiplicativity of the divisor function, we obtain

$$\prod_{j=1}^{r} \gcd(u-v,m_j) m_j^{-1} \tau(m_j)^{r^2+2r} = \gcd(u-v,m) m^{-1} \tau(m)^{r^2+2r}.$$

Therefore, for some $j \in \{1, \ldots, r\}$ we have

$$\gcd(u-v, m_j) m_j^{-1} \tau(m_j)^{r^2+2r} \le \left(\gcd(u-v, m) m^{-1} \tau(m)^{r^2+2r}\right)^{1/r},$$

and the result now follows. □

We remark that several stronger and more general results of this type have recently been given by Chang [3].

We also recall the following classical result of Deuring [4].

Lemma 4. *For any prime p and any integer t with $|t| \le 2p^{1/2}$, there is an elliptic curve E over $\mathbb{F}_p$ with $\#E(\mathbb{F}_p) = p + 1 - t$.*

3. Proof of Theorem 1

Let Q be a sufficiently large integer. We then set

$$L = \lfloor 0.3 \log Q \log\log\log Q \rfloor, \quad M = \left\lfloor \frac{\log Q}{\log\log\log Q} \right\rfloor, \quad T = \left\lfloor Q^{1/2} \right\rfloor.$$

Since, by the prime number theorem

$$\prod_{\ell \le M} \ell = Q^{o(1)},$$

we see from Lemma 4 that it is enough to show that for any sufficiently large Q, there is an integer $t \in [1, T]$ and a prime $p \in (Q/2, Q]$ such that

$$\left(\frac{t^2 - 4p}{\ell}\right) \ne 1 \tag{4}$$

for all primes $\ell \in [M, L]$.

Clearly, if the condition (4) is violated, then

$$\prod_{\ell \in [M,L]} \left(1 - \left(\frac{t^2 - 4p}{\ell}\right)\right) = 0.$$

Thus it is enough to show that the sum

$$W = \sum_{1 \le t \le T} \sum_{Q/2 < p \le Q} \prod_{\ell \in [M,L]} \left(1 - \left(\frac{t^2 - 4p}{\ell}\right)\right)$$

is positive, that is, that

$$W > 0 \tag{5}$$

for the above choice of L, M and T, provided that Q is sufficiently large.

Let $\mathcal{M}$ be the set of $2^{\pi(L)-\pi(M)}$ square-free products (including the empty product) composed of primes $\ell \in [M, L]$, and let $\mathcal{M}^* = \mathcal{M} \setminus \{1\}$. We have

$$W = \sum_{1 \le t \le T} \sum_{Q/2 < p \le Q} \sum_{m \in \mathcal{M}} \mu(m) \left(\frac{t^2 - 4p}{m}\right).$$

Changing the order of summation and separating the term $T(\pi(Q) - \pi(Q/2))$ corresponding to $m = 1$, we derive

$$W = T(\pi(Q) - \pi(Q/2)) + \sum_{m \in \mathcal{M}^*} \mu(m) S(m), \tag{6}$$

where

$$S(m) = \sum_{1 \le t \le T} \sum_{Q/2 < p \le Q} \left(\frac{t^2 - 4p}{m} \right).$$

We have

$$|S(m)| \le \sum_{Q/2 < p \le Q} \left| \sum_{1 \le t \le T} \left(\frac{t^2 - 4p}{m} \right) \right|.$$

For $m \le T^{1/4}$ we use Lemma 2 (clearly, we can assume that Q is large enough so that $M > 2$ and thus m is odd). We also note that

$$C^{\omega(m)} = \tau(m)^{\log C / \log 2} = m^{o(1)},$$

where C is the constant of Lemma 2, so we obtain

$$S(m) \ll \pi(Q) \left(T/m + C^{\omega(m)} m^{1/2} \log m \right) \ll \pi(Q) T/m.$$

Thus for the contribution from all such sums we derive

$$\sum_{\substack{m \in \mathcal{M}^* \\ m \le T^{1/4}}} |S(m)| \ll \pi(Q) T \sum_{\substack{m \in \mathcal{M}^* \\ m \le T^{1/4}}} 1/m \ll \pi(Q) T \left(\prod_{\ell \in [M,L]} \left(1 + \frac{1}{\ell}\right) - 1 \right). \tag{7}$$

Furthermore,

$$\log \prod_{\ell \in [M,L]} \left(1 + \frac{1}{\ell}\right) = \sum_{\ell \in [M,L]} \log \left(1 + \frac{1}{\ell}\right) \ll \sum_{\ell \in [M,L]} \frac{1}{\ell}.$$

By the Mertens theorem, see [6, Equation (2.15)],

$$\begin{aligned} \sum_{\ell \in [M,L]} \frac{1}{\ell} &= \log \frac{\log L}{\log M} + O(1/\log M) \\ &= \log \frac{\log \log Q + \log \log \log \log Q + \log 0.3}{\log \log Q - \log \log \log \log Q} + O(1/\log M) \\ &= \log \left(1 + O\left(\frac{\log \log \log \log Q}{\log \log Q} \right) \right) + O(1/\log M) \\ &\ll \frac{\log \log \log \log Q}{\log \log Q}. \end{aligned}$$

Therefore,

$$\prod_{\ell \in [M,L]} \left(1 + \frac{1}{\ell}\right) = 1 + O\left(\frac{\log \log \log \log Q}{\log \log Q} \right).$$

Inserting this bound in (7), we obtain

$$\sum_{\substack{m \in \mathcal{M}^* \\ m \le T^{1/4}}} |S(m)| \ll \pi(Q) T \frac{\log \log \log \log Q}{\log \log Q} = o(\pi(Q) T). \tag{8}$$

To estimate the sums $S(m)$ for $m > T^{1/4}$, using the Cauchy inequality and then extending the summation range over all positive integers $n \le 4Q$, we derive

$$
\begin{aligned}
|S(m)|^2 &\le (\pi(Q) - \pi(Q/2)) \sum_{Q/2<p\le Q} \left| \sum_{1\le t\le T} \left(\frac{t^2-4p}{m} \right) \right|^2 \\
&\le \pi(Q) \sum_{n\le 4Q} \left| \sum_{1\le t\le T} \left(\frac{t^2-n}{m} \right) \right|^2 \\
&= \pi(Q) \sum_{1\le s,t\le T} \sum_{n\le 4Q} \left(\frac{(s^2-n)(t^2-n)}{m} \right).
\end{aligned}
$$

If $\gcd(s^2-t^2, m) > m^{1/2}$, we estimate the inner sum trivially as $O(Q)$. The total contribution from such pairs (s,t) is at most

$$
\begin{aligned}
\sum_{\substack{d|m \\ d>m^{1/2}}} \sum_{\substack{1\le s,t\le T \\ s^2\equiv t^2 \pmod d}} 1 &\le \sum_{\substack{d|m \\ d>m^{1/2}}} T\,(T/d+1)\,2^{\omega(d)} \\
&\le T\left(T/m^{1/2}+1\right)\tau(m)^2,
\end{aligned} \tag{9}
$$

since for a square-free d, by the Chinese remainder theorem, any quadratic congruence of the form $s^2 \equiv a \pmod d$, $1 \le s \le d$, has at most $2^{\omega(d)}$ solutions.

If $\gcd(s^2-t^2, m) \le m^{1/2}$, we apply Lemma 3 to the inner sum, getting

$$
\begin{aligned}
&\left| \sum_{n\le 4Q} \left(\frac{(s^2-n)(t^2-n)}{m} \right) \right| \\
&\qquad \le 16Q \left(\gcd(s^2-t^2, m) m^{-1} \tau(m)^{r^2+2r} \right)^{1/(r2^r)} \\
&\qquad \le 16Q \left(m^{-1/2} \tau(m)^{r^2+2r} \right)^{1/(r2^r)}
\end{aligned} \tag{10}
$$

for any positive integer r with

$$
(4Q)^r > m^3. \tag{11}
$$

Therefore, combining (9) and (10), we obtain

$$
\begin{aligned}
S(m)^2 \ll\ & \pi(Q)QT\left(T/m^{1/2}+1\right)\tau(m)^2 \\
&+ \pi(Q)QT^2\left(m^{-1/2}\tau(m)^{r^2+2r}\right)^{1/(r2^r)}.
\end{aligned} \tag{12}
$$

Furthermore, for $m \in \mathcal{M}$ we have

$$
\tau(m) \le 2^{\pi(L)} = \exp\left((\log 2 + o(1)) \frac{\log Q \log\log\log Q}{\log\log Q} \right). \tag{13}
$$

So if

$$
r^2 + 2r \le 0.01 \frac{\log\log Q}{\log\log\log Q}, \tag{14}
$$

then for $m > T^{1/4}$ we have

$$
\tau(m)^{r^2+2r} \le Q^{0.01\log 2+o(1)} = T^{0.02\log 2+o(1)} \le m^{0.08\log 2+o(1)} \le m^{1/6},
$$

provided that Q is large enough. Hence,

$$m^{-1/2}\tau(m)^{r^2+2r} \le m^{-1/3} \le T^{-1/12}.$$

Furthermore, since (13) implies that $\tau(m) = T^{o(1)}$ for $m \in \mathcal{M}$, we see that (12) implies that for $m > T^{1/4}$, for any r satisfying (11) and (14), we have

$$S(m) \ll QT^{1-1/(24r2^r)}.$$

Therefore,

$$\sum_{\substack{m\in\mathcal{M}^* \\ m>T^{1/4}}} |S(m)| \ll 2^{\pi(L)}QT^{1-1/(24r2^r)}$$

$$\le QT^{1-1/(24r2^r)} \exp\left((\log 2 + o(1))\frac{\log Q \log\log\log Q}{\log\log Q}\right).$$

In particular, if we set

$$r = \lfloor \log\log\log Q \rfloor$$

then

$$T^{1/(24r2^r)} = \exp\left(\frac{\log Q}{(\log\log Q)^{\log 2 + o(1)}}\right).$$

Therefore,

$$\sum_{\substack{m\in\mathcal{M}^* \\ m>T^{1/4}}} |S(m)| \ll QT^{1-1/(25r2^r)} = o(\pi(Q)T). \tag{15}$$

It is also obvious that (14) is satisfied for the above choice of r. Furthermore, the condition (11) is satisfied as well because

$$(4Q)^r \ge \exp((1+o(1))\log Q \log\log\log Q)$$

and

$$\max_{m\in\mathcal{M}} m = \exp((1+o(1))L) = \exp((0.3+o(1))\log Q \log\log\log Q).$$

Substituting (8) and (15) in (6), we see that (5) holds, which concludes the proof.

Acknowledgements

The author is very grateful to Takakazu Satoh and Andrew Sutherland for very useful comments. The author would also like to thank the anonymous referee for the careful reading of the original manuscript and helpful suggestions.

During the preparation of this work the author was supported in part by Australian Research Council Grant DP130100237, and Macquarie University Grant MQRDG1465020.

References

[1] R. Avanzi, H. Cohen, C. Doche, G. Frey, T. Lange, K. Nguyen and F. Vercauteren, *Elliptic and hyperelliptic curve cryptography: Theory and practice*, CRC Press, 2005.

[2] Stephan Baier and Liangyi Zhao, *On primes in quadratric progressions*, Int. J. Number Theory **5** (2009), no. 6, 1017–1035, DOI 10.1142/S1793042109002523. MR2569742 (2010k:11147)

[3] Mei-Chu Chang, *Short character sums for composite moduli*, J. Anal. Math. **123** (2014), 1–33, DOI 10.1007/s11854-014-0012-y. MR3233573

[4] Max Deuring, *Die Typen der Multiplikatorenringe elliptischer Funktionenkörper* (German), Abh. Math. Sem. Hansischen Univ. **14** (1941), 197–272. MR0005125 (3,104f)

[5] Noam D. Elkies, *Elliptic and modular curves over finite fields and related computational issues*, Computational perspectives on number theory (Chicago, IL, 1995), AMS/IP Stud. Adv. Math., vol. 7, Amer. Math. Soc., Providence, RI, 1998, pp. 21–76. MR1486831 (99a:11078)

[6] Henryk Iwaniec and Emmanuel Kowalski, *Analytic number theory*, American Mathematical Society Colloquium Publications, vol. 53, American Mathematical Society, Providence, RI, 2004. MR2061214 (2005h:11005)

[7] Guang Shi Lü and Hai Wei Sun, *Prime in quadratic progressions on average*, Acta Math. Sin. (Engl. Ser.) **27** (2011), no. 6, 1187–1194, DOI 10.1007/s10114-011-8059-5. MR2795366 (2012j:11182)

[8] Florian Luca and Igor E. Shparlinski, *On quadratic fields generated by polynomials*, Arch. Math. (Basel) **91** (2008), no. 5, 399–408, DOI 10.1007/s00013-008-2656-2. MR2461203 (2010c:11119)

[9] Hugh L. Montgomery and Robert C. Vaughan, *Multiplicative number theory. I. Classical theory*, Cambridge Studies in Advanced Mathematics, vol. 97, Cambridge University Press, Cambridge, 2007. MR2378655 (2009b:11001)

[10] Takakazu Satoh, *On p-adic point counting algorithms for elliptic curves over finite fields*, Algorithmic number theory (Sydney, 2002), Lecture Notes in Comput. Sci., vol. 2369, Springer, Berlin, 2002, pp. 43–66, DOI 10.1007/3-540-45455-1_5. MR2041073 (2004k:11098)

[11] René Schoof, *Elliptic curves over finite fields and the computation of square roots mod p*, Math. Comp. **44** (1985), no. 170, 483–494, DOI 10.2307/2007968. MR777280 (86e:11122)

[12] Igor E. Shparlinski and Andrew V. Sutherland, *On the distribution of Atkin and Elkies primes*, Found. Comput. Math. **14** (2014), no. 2, 285–297, DOI 10.1007/s10208-013-9181-9. MR3179585

[13] Joseph H. Silverman, *The arithmetic of elliptic curves*, 2nd ed., Graduate Texts in Mathematics, vol. 106, Springer, Dordrecht, 2009. MR2514094 (2010i:11005)

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

Current address: Department of Pure Mathematics, University of New South Wales, Sydney, NSW 2052, Australia
E-mail address: igor.shparlinski@unsw.edu.au