On the Product of Small Elkies Primes

Igor E. Shparlinski
Department of Computing
Macquarie University
Sydney, NSW 2109, Australia
igor.shparlinski@mq.edu.au

January 3, 2013

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. These primes are used in the presently most efficient algorithm to compute $\#E(\mathbb{F}_q)$. In particular, the bound $L_q(E)$ such that the product of all Elkies primes for E up to $L_q(E)$ 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 results of Galbraith and Satoh (2002), conditional under the Generalised Riemann Hypothesis, and of Shparlinski and Sutherland (2012), 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, 12] for a background on elliptic curves. 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,

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

where $\pi(L)$ 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, naive heuristic 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 derives 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 [5, Section 5.9] or [8, 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 [11] 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 that those implied by the GRH. In particular, Let $\mathcal{L}_E(p)$ be the set all Elkies primes for an elliptic curve E over $\mathbb{F}_p$. We see that the prime number theorem and the result of [11] 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 for 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 for 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 $c > 0$ so that for infinitely many pairs (p, E) of primes p and curves E over $\mathbb{F}_p$, and $L \le c \log p \log\log\log p$ we have*

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

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 to replace $\log p \log\log\log p$ with $\log p \log\log p$ in Theorem 1. Unfortunately, presently the required representation $n = 4p - t^2$ is known to exist only for almost all n (see [2, 6]), 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 $|U| \le cV$ 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 [5, Section 3.5]. We also use $\tau(k)$ and $\mu(k)$ to denote the number of integer positive 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 [7, Lemma 2.2] and is also given in [11].

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 $C \geq 1$.

We also need a slight extension of [5, 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 [5, Theorem 12.10], implies the following results"

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

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

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

Proof. As in the proof of [5, Corollary 12.14], we note that there is a factorisation

$$m = m_1 \ldots m_r$$

with $m_j \leq N^{4/9}$, $j = 1, \ldots, r$. In particular, by [5, Theorem 12.10], recalling (3), we see that for any $j = 1, \ldots, r$ we have

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

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

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

and the result now follows. $\square$

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

Furthermore, we also recall the following classical results of Deuring [4].

Lemma 4. *For any prime p and an integer t with $|t| \le 2q^{1/2}$, there is a 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

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

Since, by the prime number theorem

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

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

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

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

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

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 out of primes $\ell \in [M, L]$, and let $\mathcal{M}^* = \mathcal{M} \setminus \{1\}$. We have

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

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

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

Thus

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

For $m \le T^{1/4}$ we use Lemma 2 and note that

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

so we obtain

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

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 [5, 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 integers $n \le 4Q$, we derive

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

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

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

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

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

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

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

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

$$\tau(m)^{r^2+2r} \le Q^{0.01\log 2+o(1)} = T^{0.01\log 2+o(1)} \le m^{0.04\log 2+o(1)} \le m^{1/6},$$

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,

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

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

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,

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

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.

Acknowledgement

The author is very grateful to Andrew Sutherland for very useful comments.

During the preparation of this work the author was supported in part by the Australian Research Council grant DP1092835, 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] S. Baier and L. Zhao, 'On primes in quadratric progressions', *Int. J. Number Theory*, **5** (2009), 1017–1035.

[3] M.-C. Chang, 'Short character sums for composite moduli', *Preprint*, 2011 (available from `http://arxiv.org/abs/1201.0299`).

[4] M. Deuring, 'Die Typen der Multiplikatorenringe elliptischer Funktionenkörper', *Abh. Math. Sem. Hansischen Univ.*, **14** (1941), 197–272.

[5] H. Iwaniec and E. Kowalski, *Analytic number theory*, Amer. Math. Soc., Providence, RI, 2004.

[6] G. S., Lü, and H. W. Sun, 'Prime in quadratic progressions on average', *Acta Math. Sin. (Engl. Ser.)*, **27** (2011), 1187–1194.

[7] F. Luca and I. E. Shparlinski, 'On quadratic fields generated by polynomials', *Arch. Math.*, **91** (2008), 399–408.

[8] H. L. Montgomery and R. C. Vaughan, *Multiplicative number theory I: Classical theory*, Cambridge Univ. Press, Cambridge, 2006.

[9] M. Rabin, 'Probabilistic algorithms for testing primality', *J. Number Theory*, **12** (1980), 128–138.

[10] T. Satoh, 'On p-adic point counting algorithms for elliptic curves over finite fields', *Lect. Notes in Comp. Sci.*, Springer-Verlag, Berlin, **2369** (2002), 43–66.

[11] I. E. Shparlinski and A. V. Sutherland, 'On the distribution of Atkin and Elkies primes', *Preprint*, 2011 (available from `http://arxiv.org/abs/1112.3390`).

[12] J. H. Silverman, *The arithmetic of elliptic curves*, 2nd ed., Springer, Dordrecht, 2009.