ON PSEUDOPOINTS OF ALGEBRAIC CURVES

REZA R. FARASHAHI AND IGOR E. SHPARLINSKI

Abstract. Following Kraitchik and Lehmer, we say that a positive integer \( n \equiv 1 \pmod{8} \) is an \( x \)-pseudosquare if it is a quadratic residue for each odd prime \( p \leq x \), yet is not a square. We extend this definition to algebraic curves and say that \( n \) is an \( x \)-pseudopoint of a curve \( f(u, v) = 0 \) (where \( f \in \mathbb{Z}[U, V] \)) if for all sufficiently large primes \( p \leq x \) the congruence \( f(n, m) \equiv 0 \pmod{p} \) is satisfied for some \( m \).

We use the Bombieri bound of exponential sums along a curve to estimate the smallest \( x \)-pseudopoint, which shows the limitations of the modular approach to searching for points on curves.

1. Introduction

Following Lehmer in [9], given a real \( x \geq 1 \), we say that a nonsquare positive integer \( n \) is an \( x \)-pseudosquare if \( n \equiv 1 \pmod{8} \) and \( (n/p) = 1 \) for each odd prime \( p \leq x \), see also [13, 15, 16, 17] for further results. Here we generalise this notion and introduce and study \( x \)-pseudopoints on algebraic curves.

More precisely, given an absolutely irreducible polynomial \( f(U, V) \in \mathbb{Z}[U, V] \) and an integer \( q \geq 1 \) we denote

\[(1) \quad \mathcal{Z}_f(q) = \{(n, m) : 0 \leq n, m < q, f(n, m) \equiv 0 \pmod{q}\}.\]

Then, we define \( \mathcal{P}_f \) as the set of primes \( p \) for which \( \mathcal{Z}_f(p) \) is not empty. We note that an absolutely irreducible polynomial \( f \) remains absolutely irreducible modulo all sufficiently large prime numbers \( p \) by Ostrowski [11]. Therefore, by the Weil bound, see [10, Section VIII.5, Bound (5.7)], we conclude that \( \mathcal{P}_f \) contains all sufficiently large primes. In particular, for

\[M_f(x) = \prod_{p \in \mathcal{P}_f(x)} p\]

by the prime number theorem, we have

\[(2) \quad M_f(x) = \exp((1 + o(1))x).\]
Furthermore for a real $x \geq 1$, we denote by $\mathcal{P}_f(x) = \mathcal{P}_f \cap [2, x]$ and say that an integer $n \geq 0$ is an $x$-pseudopoint of $f$ if for all $p \in \mathcal{P}_f(x)$ we have $(n, m) \in \mathbb{Z}_f(p)$ for some $m$, but the equation $f(n, m) = 0$ has no integer solution $m \in \mathbb{Z}$. We note that Bernstein \cite{Bernstein2} has introduced and studied this notion in the case of the polynomials of the form $f(U, V) = g(U) - V^2$.

Clearly, apart of the congruence condition $n \equiv 1 \pmod{8}$ and the coprimality condition $\gcd(n, p) = 1$ for primes $p \leq x$, the polynomial $f(U, V) = U - V^2$ corresponds to the case of $x$-pseudosquares.

It is easy to show that for any absolutely irreducible polynomial $f(U, V) \in \mathbb{Z}[U, V]$ nonlinear in $V$, that is, $\deg_V f \geq 2$, the smallest $x$-pseudopoint $N_f(x)$ satisfies the bound

$$N_f(x) = O(M_f(x)) = \exp((1 + o(1))x).$$

Clearly the condition of nonlinearity in $V$ is necessary (for example, the polynomial $f(U, V) = U^2 - V$ does not have any pseudopoints).

Indeed, the bound \cite{Bernstein2} can be derived from the Chinese remaindering theorem combined with the Weil bound (see \cite{Weil} Section VIII.5, Bound (5.7)), and also the bound of Bombieri and Pila \cite{BombieriPila} on the number of integer points on plane curves.

Here we use the Bombieri bound \cite{Bombieri} to improve \cite{Bernstein2}.

**Theorem 1.** For any absolutely irreducible polynomial

$$f(U, V) \in \mathbb{Z}[U, V]$$

that is nonlinear in $V$, that is,

$$\deg_V f \geq 2,$$

we have

$$N_f(x) \leq M_f(x)^{1/2+o(1)}.$$

The bound of Theorem \cite{Bombieri} is an analogues of similar, albeit stronger, estimates for pseudosquares, see \cite{BombieriPila1, BombieriPila2}. Besides it shows the limitations of the modular approach to searching for points on curves. Indeed, assuming that $\mathcal{P}_f$ consists of all primes (otherwise the equation $f(n, m) = 0$ has no integer solutions), we see that there is a reasonably small point which is a solution to the corresponding congruence modulo all small primes but is not a solution to the equation.

2. **Preparations**

We need some background on exponential sums and congruences. For an integer $q$ and a complex $z$, we denote

$$e_q(z) = \exp(2\pi i z / q)$$
and recall the identity
\begin{equation}
\frac{1}{q} \sum_{-q/2 < a \leq q/2} e\left(\frac{an}{q}\right) = \begin{cases} 
1, & \text{if } n \equiv 0 \pmod{q}, \\
0, & \text{if } n \not\equiv 0 \pmod{q},
\end{cases}
\end{equation}
which follows from the formula for the sum of geometric progression.

We also need the following bound
\begin{equation}
\sum_{n=1}^{N} e\left(\frac{an}{q}\right) = O\left(\min\{N, q/|a|\}\right),
\end{equation}
which holds for any integers \( a \) and \( N \geq 1 \) with \( 0 < |a| \leq q/2 \), see [7, Bound (8.6)].

Our main tool is the following special case of the Bombieri bound [3, Theorem 6] of exponential sums along a curve.

**Lemma 2.** Assume that for a prime \( p \), a polynomial \( f(U, V) \in \mathbb{Z}[U, V] \) is such that its reduction modulo \( p \) does not have a factor of the form \( U - \alpha \) with some \( \alpha \in \mathbb{F}_p \). Then uniformly over \( a \in \mathbb{Z} \) with \( \gcd(a, p) = 1 \)
\begin{equation}
\sum_{(u,v) \in \mathbb{Z}_Mf(x)} e_p(au) = O(p^{1/2}),
\end{equation}
where the implied constant depends only on \( \deg f \).

Finally, we need the following consequence of the Chinese remainder theorem (see also [7, Equation (12.21)] for a very similar statement).

**Lemma 3.** For any polynomial
\( f(U, V) \in \mathbb{Z}[U, V] \),
we have
\begin{equation}
\sum_{(u,v) \in \mathbb{Z}_f(Mf(x))} e_{Mf(x)}(au) = \prod_{p \in \mathcal{P}_f(x)} \sum_{(u,v) \in \mathbb{Z}_p} e_p(au).
\end{equation}

**Proof.** Let \( \mathbb{Z}_m \) denote the residue ring modulo \( m \). From the Chinese remainder theorem, there is a bijection
\begin{equation}
\mathbb{Z}_{Mf(x)} \simeq \bigotimes_{p \in \mathcal{P}_f(x)} \mathbb{Z}_p
\end{equation}
by \( u \mapsto (u_p)_{p \in \mathcal{P}_f(x)} \). On the other hand, every tuple \( (u_p)_{p \in \mathcal{P}_f(x)} \) corresponded to the unique element
\begin{equation}
u = \sum_{p \in \mathcal{P}_f(x)} \frac{M_f(x)}{p} u_p \in \mathbb{Z}_{Mf(x)}.
\end{equation}
Then,
\[ e_{M_f(x)}(au) = \prod_{p \in \mathcal{P}_f(x)} e_p(au_p). \]
Moreover, in a natural way (6) yields a bijection between the points
\((u, v)\) in \(\mathbb{Z}_f(M_f(x))\) and the tuples of points
\[ ((u_p, v_p))_{p \in \mathcal{P}_f(x)} \in \bigotimes_{p \in \mathcal{P}_f(x)} \mathbb{Z}_f(p). \]
Therefore,
\[ \sum_{(u,v) \in \mathbb{Z}_f(M_f(x))} e_{M_f(x)}(au) = \sum_{((u_p,v_p))_{p \in \mathcal{P}_f(x)}} \prod_{p \in \mathcal{P}_f(x)} e_p(au_p) \]
\[ = \prod_{p \in \mathcal{P}_f(x)} \sum_{(u,v) \in \mathbb{Z}_f(p)} e_p(au), \]
which completes the proof.

\[ \square \]

**Lemma 4.** For any absolutely irreducible polynomial
\[ f(U, V) \in \mathbb{Z}[U, V], \]
there is a constant \(c > 0\), depending only on \(f\) such that
\[ \prod_{p \in \mathcal{P}_f(x)} (p + cp^{1/2}) \geq \# \mathbb{Z}_f(M_f(x)) \geq \prod_{p \in \mathcal{P}_f(x)} \max\{1, p - cp^{1/2}\}. \]

**Proof.** By the Chinese remaindering theorem we have a bijection between points of \(\mathbb{Z}_f(M_f(x))\) and tuples of points in \(\prod_{p \in \mathcal{P}_f(x)} \mathbb{Z}_f(p)\), see the proof of Lemma 3. Therefore,
\[ \# \mathbb{Z}_f(M_f(x)) = \prod_{p \in \mathcal{P}_f(x)} \# \mathbb{Z}_f(p). \]
As we have noted, the polynomial \(f\) remains absolutely irreducible modulo all sufficiently large prime numbers \(p\) by Ostrowski [11]. Let \(c_f\) be the least integer such that \(f\) is absolutely irreducible over \(\mathbb{Z}_p\) for all prime numbers \(p \geq c_f\) (for explicit bounds on \(c_f\) see for example [6, 14, 18]). If \(f\) is absolutely irreducible over \(\mathbb{Z}_p\), and \(p \geq c_f\) then from the Weil bound we have
\[ (7) \quad \# \mathbb{Z}_f(p) = p + O(p^{1/2}), \]
see [11] Section VIII.5, Bound (5.7)]. Furthermore, allowing the implied constant in (7) to depend of \(f\), we see that (7) trivially holds for all primes \(p\). By definition, for all \(p \in \mathcal{P}_f(x)\) we have \(\# \mathbb{Z}_f(p) \geq 1\), which completes the proof. \(\square\)
Corollary 5. For any absolutely irreducible polynomial
\[ f(U, V) \in \mathbb{Z}[U, V], \]
we have
\[ \#Z_f(M_f(x)) = M_f(x)^{1+o(1)}. \]

Proof. Since
\[ p \exp(c_0 p^{-1/2}) \geq p + cp^{1/2} \geq \max\{1, p - cp^{1/2}\} \]
\[ \geq p \exp(-c_0 p^{-1/2}) \]
for an appropriate constant \( c_0 \geq 0 \), we have
\[ \#Z_f(M_f(x)) = M_f(x) \exp\left( O\left( \sum_{p \leq x} p^{-1/2} \right) \right) \]
\[ = M_f(x) \exp\left( O(x^{1/2}/\log x) \right), \]
which together with (2) implies the result. \( \square \)

Finally we need the following estimate on the number of points on a curve with a restricted coordinate which follows from a result of Pila [12] that in turn slightly improves the previous estimate of Bombieri and Pila [4].

Lemma 6. For any absolutely irreducible polynomial
\[ f(U, V) \in \mathbb{Z}[U, V] \]
nonlinear in \( V \) that is,
\[ \deg_V f \geq 2 \]
the equation
\[ f(n, m) = 0, \quad 0 \leq n < N, \ m \in \mathbb{Z}, \]
has at most \( O(N^{1/2+o(1)}) \) solutions.

Proof. Let \( d = \deg f \). Since \( \deg_V f \geq 2 \) we see that for any solution to the above equation we have \( m = O(n^{d/2}) = O(N^{d/2}) \). Recalling that by [12], an absolutely irreducible polynomial of degree \( d \) has \( O(T^{1/d+o(1)}) \) solutions in a box \([0, T] \times [0, T]\) (where the implied constants depend only on \( d \)), we derive the result. \( \square \)
3. Proof of Theorem 1

Let \( T_f(N; x) \) be the number of solutions \((n, m)\) to the congruence
\[
(8) \quad f(n, m) \equiv 0 \pmod{M_f(x)}, \quad 0 \leq n < N, \ 0 \leq m < M_f(x).
\]

Using (4), we write
\[
T_f(N; x) = \sum_{(n,m) \in \mathbb{Z}_f(M_f(x))} \sum_{k=0}^{N-1} \frac{1}{M_f(x)} e_{M_f(x)}(a(n - k))
\]
\[
= \frac{1}{M_f(x)} \sum_{-M_f(x)/2 < a \leq M_f(x)/2} e_{M_f(x)}(an) \sum_{k=0}^{N-1} e_{M_f(x)}(-ak).
\]

Separating the term corresponding to \( a = 0 \), and recalling (5), we obtain
\[
(9) \quad T_f(N; x) - \frac{N}{M_f(x)} \# \mathbb{Z}_f(M_f(x)) = O(R_f(N; x)),
\]
where, as before, \( \mathbb{Z}_f(q) \) is defined by (1) and
\[
R_f(N; x) = \sum_{0 < |a| \leq M_f(x)/2} \frac{1}{|a|} \left| \sum_{(n,m) \in \mathbb{Z}_f(M_f(x))} e_{M_f(x)}(an) \right|.
\]

To estimate \( R_f(N; x) \), for every \( d \mid M_f(x) \), we collect together the values of \( a \) with the same value \( \gcd(a, M_f(x)) = d \) and write them as \( a = db \), getting
\[
R_f(N; x) = \sum_{d \mid M_f(x)} \frac{1}{d} \sum_{0 < |b| \leq M_f(x)/2d} \frac{1}{|b|} \left| \sum_{(n,m) \in \mathbb{Z}_f(M_f(x))} e_{M_f(x)}(dbm) \right|.
\]

Recalling Lemma 3 and then estimating the corresponding exponential sums via Lemma 2 for \( p \nmid d \) (and using the trivial bound \( \# \mathbb{Z}_f(p) \) for \( p \mid d \)), we deduce
\[
\left| \sum_{(n,m) \in \mathbb{Z}_f(M_f(x))} e_{M_f(x)}(dbm) \right| \leq C^x(M_f(x)/d)^{1/2}d = C^x(M_f(x)d)^{1/2},
\]
where $C$ is the implied constant of Lemma 2 and, as usual, $\pi(x)$ is the number of primes $p \leq x$. Therefore, using (2)

$$R_f(N; x) \leq C^{\pi(x)} \sum_{d|M_f(x)} \frac{1}{d} \sum_{\substack{0 < |b| \leq M_f(x)/2d \\ \gcd(b, M_f(x)/d) = 1}} \frac{(M_f(x)d)^{1/2}}{|b|}$$

$$= C^{\pi(x)} M_f(x)^{1/2} \sum_{d|M_f(x)} \frac{1}{d^{1/2}} \sum_{\substack{0 < |b| \leq M_f(x)/2d \\ \gcd(b, M_f(x)/d) = 1}} \frac{1}{|b|}$$

$$= O \left( (2C)^{\pi(x)} M_f(x)^{1/2} \log M_f(x) \right) = O \left( M_f(x)^{1/2+o(1)} \right),$$

as trivially

$$\sum_{d|M_f(x)} \frac{1}{d^{1/2}} \leq \sum_{d|M_f(x)} 1 \leq 2^{\pi(x)}.$$

Thus, we see from (9) that

$$\left| T_f(N; x) - \frac{N}{M_f(x)} \# \mathcal{Z}_f(M_f(x)) \right| \leq M_f(x)^{1/2+o(1)}.$$

Furthermore, by Corollary 4 we see that for any fixed $\varepsilon > 0$, taking $N = \lceil M_f(x)^{1/2+\varepsilon} \rceil$ we obtain

$$T_f(N; x) = N^{1+o(1)}.$$

By the Chinese remaindering theorem we see that for every fixed $n$ there are no more that $d^{\pi(x)}$ solutions $m$ to the congruence $f(n, m) \equiv 0 \pmod{M_f(x)}$, $0 \leq m < M_f(x)$. Thus we have at least

$$T_f(N; x) d^{-\pi(x)} = T_f(N; x) M_f(x)^{o(1)} = N^{1+o(1)},$$

values of $n$ for which the congruence $f(n, m) \equiv 0 \pmod{M_f(x)}$, has a solution. Using Lemma 6 we see that there is a solution $(n, m)$ to (8) with $f(n, m) \neq 0$. Since $\varepsilon$ is arbitrary, this concludes the proof.

4. Comments

It is easy to see that all implicit constants in our estimates can be efficiently evaluated. For example, see [6, 14, 18] for explicit versions of the Ostrowski theorem.

We remark that besides pseudosquares, in a number of works [11, 5, 18] the notion of pseudopowers has been studied. Namely, following Bach, Lukes, Shallit and Williams [11], we say that an integer $n > 0$ is an $x$-pseudopower to base $g$ (for a given integer $g$ with $|g| \geq 2$) if $n$ is not a power of $g$ over the integers but is a power of $g$ modulo all primes
$p \leq x$, that is, if for all primes $p \leq x$ there exists an integer $k_p \geq 0$ such that $n \equiv g^{k_p} \pmod{p}$.

The notion of pseudopowers naturally extends to elliptic curves. More precisely, given an elliptic curve $E$ over $\mathbb{Q}$ and a rational point $P \in E(\mathbb{Q})$ we say that $Q$ is an $x$-pseudomultiple of $P$ if for every prime $p \leq x$ at which $E$ has good reduction, there is an integer $k_p \geq 0$ so that $Q \equiv k_p P \pmod{p}$ but $Q$ is not of the form $Q = kP + T$ for some integer $k$ and some torsion point $T$. Clearly $E$ has to be of rank at least 2 for $x$-pseudomultiple to exist. Obtaining upper bounds on the canonical height of the smallest pseudopowers is a natural and challenging questions.

Acknowledgements.

The authors are grateful to Joe Silverman for the idea of the question on $x$-pseudomultiples on elliptic curves in Section 4; in fact this also gave us the idea of defining and studying $x$-pseudopoints on curves.

Both authors were supported in part by ARC Grant DP0881473.

References

[1] E. Bach, R. Lukes, J. Shallit and H. C. Williams, ‘Results and estimates on pseudopowers’, Math. Comp., 65 (1996), 1737–1747.
[2] D. J. Bernstein, ‘Doubly focused enumeration of locally square polynomial values’, High Primes and Misdemeanours: Lectures in Honour of the 60th Birthday of Hugh Cowie Williams, Fields Institute Communications, vol.41, Amer. Math. Soc., 2004, 69–76.
[3] E. Bombieri, ‘On exponential sums in finite fields’, Amer. J. Math., 88 (1966), 71–105.
[4] E. Bombieri and J. Pila, ‘The number of integral points on arcs and ovals’, Duke Math. J., 59 (1989), 337–357.
[5] J. Bourgain, S. Konyagin, C. Pomerance and I. E. Shparlinski, ‘On the smallest pseudopower’, Acta Arith., 140 (2009), 43–55.
[6] S. Gao and V. M. Rodrigues, ‘Irreducibility of polynomials modulo $p$ via Newton polytopes’, Journal of Number Theory, 101 (2003), 32–47.
[7] H. Iwaniec and E. Kowalski, Analytic number theory, Colloquium Pubs., Vol. 53, Amer. Math. Soc., Providence, RI, 2004.
[8] S. V. Konyagin, C. Pomerance, and I. E. Shparlinski, ‘On the distribution of pseudopowers’, Can. J. Math., (to appear).
[9] D. H. Lehmer, ‘A sieve problem on “pseudo-squares”’, Math. Tables and Other Aids to Computation, 8 (1954), 241–242.
[10] D. Lorenzini, An invitation to arithmetic geometry, Amer. Math. Soc., 1996.
[11] A. Ostrowski, ‘Zur arithmetischen theorie der algebraischen grösseen’, Nachr. K. Ges. Wiss. Göttingen (1919), 273–298.
[12] J. Pila, ‘Density of integer points on plane algebraic curves, Intern. Math. Research Notices, 18 (1996), 903–912.
[13] C. Pomerance, and I. E. Shparlinski, ‘On pseudosquares and pseudopowers’, *Combinatorial Number Theory, Proc. of Integers Conf. 2007*, Walter de Gruyter, Berlin, 2009, 171–184.

[14] W. M. Ruppert, ‘Reducibility of polynomials $f(x; y)$ modulo $p$’, *J. Number Theory*, **77** (1999), 62–70.

[15] A. Schinzel, ‘On pseudosquares’, *New trends in probability and statistics, Palanga, 1996*, Vol. 4, 213–220, VSP, Utrecht, 1997.

[16] J. P. Sorenson, ‘The pseudosquares prime sieve’, *Proc. 7th Algorithmic Number Theory Symp.*, Lect. Notes in Comput. Sci., vol. 4076, Springer-Verlag, Berlin, 2006, 193–207.

[17] K. Wooding and H. C. Williams, ‘Doubly-focused enumeration of pseudosquares and pseudocubes’, *Proc. 7th Algorithmic Number Theory Symp.*, Lect. Notes in Comput. Sci., vol. 4076, Springer-Verlag, Berlin, 2006, 208–211.

[18] U. Zannier, ‘On the reduction modulo $p$ of an absolutely irreducible polynomial $f(x; y)$’, *Arch. Math.*, **68** (1997), 129–138.

Department of Computing, Faculty of Science, Macquarie University, Sydney, NSW 2109, Australia

E-mail address: {reza,igor}@comp.mq.edu.au