Visible Points on Curves over Finite Fields

IGOR E. SHPARLINSKI
Department of Computing, Macquarie University
Sydney, NSW 2109, Australia
igor@ics.mq.edu.au
JOSÉ FELIPE VOLOCH
Department of Mathematics, University of Texas
Austin TX 78712 USA
voloch@math.utexas.edu

February 19, 2013

Abstract

For a prime p and an absolutely irreducible modulo p polynomial $f(U,V) \in \mathbb{Z}[U,V]$ we obtain an asymptotic formulas for the number of solutions to the congruence $f(x,y) \equiv a \pmod p$ in positive integers $x \leqslant X$, $y \leqslant Y$, with the additional condition $\gcd(x,y) = 1$. Such solutions have a natural interpretation as solutions which are visible from the origin. These formulas are derived on average over a for a fixed prime p, and also on average over p for a fixed integer a.

1 Introduction

Let p be a prime and let $f(U,V) \in \mathbb{Z}[U,V]$ be a bivariate polynomial with integer coefficients.

For real X and Y with $1 \leqslant X, Y \leqslant p$ and an integer a we consider the set

$$\mathcal{F}_{p,a}(X,Y) = \{(x,y) \in [1,X] \times [1,Y] \ : \ f(x,y) \equiv a \pmod p\}$$

which the set of points on level curves of $f(U,V)$ modulo p.

If the polynomial $f(x,y)-a$ is nonconstant absolutely irreducible polynomial modulo p of degree bigger than one can easily derive from the Bombieri bound [1] that

$$\#\mathcal{F}_{p,a}(X,Y) = \frac{XY}{p} + O\left(p^{1/2}(\log p)^2\right), \tag{1}$$

where the implied constant depends only on $\deg f$, see, for example, [3, 4, 9, 11].

In this paper we consider an apparently new question of studying the set

$$N_{p,a}(X,Y) = \{(x,y) \in \mathcal{F}_{p,a}(X,Y) \ : \ \gcd(x,y) = 1\}.$$

These points have a natural geometric interpretation as points on $\mathcal{F}_{p,a}(X,Y)$ which are "visible" from the origin, see [2, 6, 7, 10] and references therein for several other aspects of distribution of visible points in various regions.

We show that on average over $a = 0,\ldots,p-1$, the cardinality $N_{p,a}(X,Y)$ is close to its expected value $6XY/\pi^2 p$, whenever

$$XY \geqslant p^{3/2+\varepsilon} \tag{2}$$

for any fixed $\varepsilon > 0$ and sufficiently large p.

We then consider the dual situation, when a is fixed (in particular we take $a = 0$) but p varies through all primes up to T.

We recall $A \ll B$ and $A = O(B)$ both mean that $|A| \leqslant cB$ holds with some constant $c > 0$, which may depend on some specified set of parameters.

2 Absolute Irreducibility of Level Curves

We start with the following statement which could be of independent interest.

Lemma 1. *If $F(U,V) \in \mathbb{K}[U,V]$ is absolutely irreducible of degree n over a field $\mathbb{K}$, then $F(U,V) - a$ is absolutely irreducible for all but at most $C(n)$ elements $a \in \mathbb{K}$, where $C(n)$ depends only on n.*

Proof. The set of polynomials of degree n is parametrized by a projective space $\mathbb{P}^{s(n)}$ of dimension $s(n) = (n+1)(n+2)/2$ over $\mathbb{K}$, coordinatized by the coefficients. The subset X of $\mathbb{P}^{k(n)}$ consisting of reducible polynomials is a Zariski closed subset because it is the union of the images of the maps

$$\mathbb{P}^{s(k)} \times \mathbb{P}^{s(n-k)} \to \mathbb{P}^{s(n)}, \qquad k \leqslant n/2,$$

given by multiplying a polynomial of degree k with a polynomial of degree $n-k$. The map $t \mapsto F(U,V)-t$ describes a line in $\mathbb{P}^{s(n)}$ and by the assumption of absolutely irreducibility of F, this line is not contained in X. So, by the Bézout theorem, it meets X in at most $C(n)$ points, where $C(n)$ is the degree of X. Hence for all but at most $C(n)$ values of a, $F(U,V)-a$ is absolutely irreducible. ☐

3 Visible Points on Almost All Level Curves

Throughout this section, the implied constants in the notations $A \ll B$ and $A = O(B)$ may depend on the degree $n = \deg f$.

Theorem 2. *Let f be a polynomial with integer coefficients which is absolutely irreducible and of degree bigger than one modulo the prime p. Then for real X and Y with $1 \leqslant X, Y \leqslant p$ we have*

$$\sum_{a=0}^{p-1} \left| N_{p,a}(X,Y) - \frac{6}{\pi^2} \cdot \frac{XY}{p} \right| \ll X^{1/2} Y^{1/2} p^{3/4} \log p.$$

Proof. Let $\mathcal{A}_p$ consist of $a \in \{0, \ldots, p-1\}$ for which $f(U,V)-a$ is absolutely irreducible modulo p.

For an integer d, we define

$$M_{p,a}(d; X, Y) = \#\{(x,y) \in \mathcal{F}_{p,a}(X,Y) \mid \gcd(x,y) \equiv 0 \pmod d\}.$$

Let $\mu(d)$ denote the Möbius function. We recall that $\mu(1) = 1$, $\mu(d) = 0$ if $d \geqslant 2$ is not square-free and $\mu(d) = (-1)^{\omega(d)}$ otherwise, where $\omega(d)$ is the number of distinct prime divisors d. By the inclusion-exclusion principle, we write

$$N_{p,a}(X,Y) = \sum_{d=1}^{\infty} \mu(d) M_{p,a}(d; X, Y). \qquad (3)$$

Writing

$$x = ds \qquad \text{and} \qquad y = dt,$$

we have

$$\#M_{p,a}(d;X,Y) = \#\{(s,t) \in [1,X/d] \times [1,Y/d] \mid f(ds,dt) \equiv a \pmod p\}.$$

Thus $M_{p,a}(d;X,Y)$ is the number of points on a curve in a given box. If $a \in \mathcal{A}_p$ and $1 \leqslant d < p$ then $f(dU,dV) - a$ remains absolutely irreducible modulo p. Accordingly, we have an analogue of (1) which asserts that

$$M_{p,a}(d;X,Y) = \frac{XY}{d^2p} + O\left(p^{1/2}(\log p)^2\right). \tag{4}$$

We fix some positive parameter $D < p$ and substitute the bound (4) in (3) for $d \leqslant D$, getting

$$\begin{aligned} &N_{p,a}(X,Y) \\ &\qquad = \sum_{d \leqslant D} \left(\frac{\mu(d)XY}{d^2p} + O\left(p^{1/2}(\log p)^2\right)\right) + O\left(\sum_{d>D} M_{p,a}(d;X,Y)\right) \\ &\qquad = \frac{XY}{p} \sum_{d \leqslant D} \frac{\mu(d)}{d^2} + O\left(Dp^{1/2}(\log p)^2 + \sum_{d>D} M_{p,a}(d;X,Y)\right) \end{aligned}$$

for every $a \in \mathcal{A}_p$.

Furthermore

$$\sum_{d \leqslant D} \frac{\mu(d)}{d^2} = \sum_{d=1}^{\infty} \frac{\mu(d)}{d^2} + O(D^{-1}) = \prod_{\ell} \left(1 - \frac{1}{\ell^2}\right) + O(D^{-1}),$$

where the product is taken over all prime numbers ℓ. Recalling that

$$\prod_{\ell} \left(1 - \frac{1}{\ell^2}\right) = \zeta(2)^{-1} = \frac{6}{\pi^2},$$

see [5, Equation (17.2.2) and Theorem 280], we obtain

$$\left| N_{p,a}(X,Y) - \frac{6}{\pi^2} \cdot \frac{XY}{p} \right| \ll XY/Dp + Dp^{1/2}(\log p)^2 + \sum_{d>D} M_{p,a}(d;X,Y), \tag{5}$$

for every $a \in \mathcal{A}_p$.

We also remark that

$$\begin{aligned}\sum_{a=0}^{p-1}\sum_{d>D} M_{p,a}(d;X,Y) &= \sum_{d>D}\sum_{a=0}^{p-1} M_{p,a}(d;X,Y) \\ &= \sum_{d>D}\left\lfloor\frac{X}{d}\right\rfloor\left\lfloor\frac{Y}{d}\right\rfloor \leqslant XY\sum_{d>D}\frac{1}{d^2} \ll XY/D.\end{aligned} \tag{6}$$

Therefore, using the bounds (5) and (6), we obtain

$$\sum_{a\in\mathcal{A}_p}\left|N_{p,a}(X,Y) - \frac{6}{\pi^2}\cdot\frac{XY}{p}\right| \ll XY/D + Dp^{3/2}(\log p)^2. \tag{7}$$

For $a \notin \mathcal{A}_p$ we estimate $N_{p,a}(X,Y)$ trivially as

$$N_{p,a}(X,Y) \leqslant \min\{X,Y\}\deg f \ll \sqrt{XY}.$$

Thus by Lemma 1,

$$\sum_{a\notin\mathcal{A}_p}\left|N_{p,a}(X,Y) - \frac{6}{\pi^2}\cdot\frac{XY}{p}\right| \ll \max\{\sqrt{XY}, XY/p\} \ll \sqrt{XY}. \tag{8}$$

Combining (7) and (8) and taking $D = X^{1/2}Y^{1/2}p^{-3/4}(\log p)^{-1}$ we conclude the proof. $\square$

Corollary 3. *Let f be a polynomial with integer coefficients which is absolutely irreducible and of degree bigger than one. If $XY \geqslant p^{3/2}(\log p)^{2+\varepsilon}$ for some fixed $\varepsilon > 0$, then*

$$N_{p,a}(X,Y) = \left(\frac{6}{\pi^2} + o(1)\right)\frac{XY}{p}$$

for all but $o(p)$ values of $a = 0,\dots,p-1$.

4 Visible Points on Almost All Reductions

Throughout this section, the implied constants in the notations $A \ll B$ and $A = O(B)$ may depend on the coefficients of f.

To simplify notation we put

$$\mathcal{F}_p(X,Y) = \mathcal{F}_{p,0}(X,Y) \qquad\text{and}\qquad N_p(X,Y) = N_{p,0}(X,Y).$$

Theorem 4. *Let f be a polynomial with integer coefficients which is absolutely irreducible and of degree bigger than one. Then for real T, X and Y such that $T \geqslant 2\max(X, Y)$, we have*

$$\sum_{T/2 \leqslant p \leqslant T} \left| N_p(X, Y) - \frac{6}{\pi^2} \cdot \frac{XY}{p} \right| \ll X^{1/2} Y^{1/2} T^{3/4+o(1)},$$

where the sum is taken over all primes p with $T/2 \leqslant p \leqslant T$.

Proof. It is enough to consider T large enough so that f remains absolutely irreducible and of degree bigger than one for all $p, T/2 \leqslant p \leqslant T$. As before we have

$$\left| N_p(X, Y) - \frac{6}{\pi^2} \cdot \frac{XY}{p} \right| \ll XY/Dp + Dp^{1/2}(\log p)^2 + \sum_{d > D} M_p(d; X, Y). \quad (9)$$

where

$$M_p(d; X, Y) = \#\{(x, y) \in \mathcal{F}_p(X, Y) \mid \gcd(x, y) \equiv 0 \pmod{d}\}.$$

We also remark that

$$\begin{aligned} \sum_{T/2 \leqslant p \leqslant T} \sum_{d > D} M_p(d; X, Y) &= \sum_{d > D} \sum_{T \leqslant p \leqslant T} M_p(d; X, Y) \\ &= \sum_{d > D} \sum_{1 \leqslant s \leqslant X/d} \sum_{1 \leqslant t \leqslant Y/d} \sum_{\substack{T/2 \leqslant p \leqslant T \\ p \mid f(ds, dy)}} 1. \end{aligned} \quad (10)$$

Let $\mathcal{Z}$ be set of integer zeros of f in the relevant box, that is

$$\mathcal{Z} = \{(u, v) \in \mathbb{Z}^2 \ : 1 \leqslant x \leqslant X, 1 \leqslant y \leqslant Y, \ f(u, v) = 0\}.$$

It is easy to see that $\#\mathcal{Z} \ll \min(X, Y) \leqslant \sqrt{XY}$. Indeed, it is enough to notice that since $f(U, V)$ is absolutely irreducible, each specialization $g_y(U) = f(U, y)$ with $y \in \mathbb{Z}$ and $h_x(V) = f(x, V)$ with $x \in \mathbb{Z}$ is a nonzero polynomials in U and V, respectively. (Under extra, but generic, hypotheses, one can invoke Siegel's theorem, which gives $\#\mathcal{Z} = O(1)$ but this does not lead to an improvement in our final bound.) Denoting by $\tau(k)$ the number of integer divisors of a positive integer k, we see that for each $(u, v) \in \mathcal{Z}$ there are at most $\tau(u) = X^{o(1)}$ (see [5, Theorem 317]) pairs (d, s) of positive integers with

$ds = u$, after which there is at most one value of t. Thus for these triples (d, s, t), we estimate the inner sum over p in (10) trivially as T.

To estimate the rest of the sums, as before, we denote by $\omega(k)$ the number of prime divisors of a positive integer k and note that $\omega(k) \ll \log k$. Thus for $(u, v) \notin \mathcal{Z}$ we can estimate the inner sum over p in (10) as $\omega(|f(ds, dy)|) = (XY)^{o(1)}$. Therefore

$$\begin{aligned}
\sum_{T/2\leqslant p\leqslant T} \sum_{d>D} M_p(d; X, Y) &\leqslant \sum_{d>D} \sum_{\substack{1\leqslant s\leqslant X/d\\ 1\leqslant t\leqslant Y/d\\ (ds,dt)\in\mathcal{Z}}} \sum_{T/2\leqslant p\leqslant T} 1 + \sum_{d>D} \sum_{\substack{1\leqslant s\leqslant X/d\\ 1\leqslant t\leqslant Y/d\\ (ds,dt)\notin\mathcal{Z}}} \sum_{p|f(ds,dy)} 1\\
&\leqslant \#\mathcal{Z} X^{o(1)} T + (XY)^{o(1)} \sum_{d>D} \sum_{\substack{1\leqslant s\leqslant X/d\\ 1\leqslant t\leqslant Y/d\\ (ds,dt)\notin\mathcal{Z}}} 1\\
&= (XY)^{1/2+o(1)} T + (XY)^{1+o(1)} D^{-1}.
\end{aligned}$$

We now put everything together getting

$$\begin{aligned}
&\sum_{T/2\leqslant p\leqslant T} \left| N_p(X, Y) - \frac{6}{\pi^2} \cdot \frac{XY}{p} \right|\\
&\qquad \ll XY/D \log T + DT^{3/2} (\log T)^2 + T(XY)^{1/2+o(1)} + (XY)^{1+o(1)} D^{-1},
\end{aligned}$$

and take $D = X^{1/2} Y^{1/2} T^{-3/4}$ getting the result. □

Corollary 5. *Let f be a polynomial with integer coefficients which is absolutely irreducible and of degree bigger than one. If $XY \geqslant T^{3/2+\varepsilon}$ for some fixed $\varepsilon > 0$, that*

$$N_p(X, Y) = \left(\frac{6}{\pi^2} + o(1) \right) \frac{XY}{p}$$

for all but $o(T/\log T)$ primes $p \in [T/2, T]$.

5 Remarks

Certainly it would be interesting to obtain an asymptotic formula for $N_{p,a}(X, Y)$ which holds for every a. Even the case of $X = Y = p$ would be of interest. We remark that for the polynomial $f(U, V) = UV$ such an asymptotic formula is give in [8] and is nontrivial provided $XY \geqslant p^{3/2+\varepsilon}$ for some fixed

$\varepsilon > 0$. However the technique of [8] does not seem to apply to more general polynomials.

We remark that studying such special cases as visible points on the curves of the shape $f(U, V) = V - g(U)$ (corresponding to points a graph of a univariate polynomial) and $f(U, V) = V^2 - X^3 - rX - s$ (corresponding to points on an elliptic curve) is also of interest and may be more accessible that the general case.

Acknowledgements.

This work began during a pleasant visit by I. S. to University of Texas sponsored by NSF grant DMS-05-03804; the support and hospitality of this institution are gratefully acknowledged. During the preparation of this paper, I. S. was supported in part by ARC grant DP0556431.

References

[1] E. Bombieri, 'On exponential sums in finite fields', *Amer. J. Math.*, **88** (1966), 71–105.

[2] F. P. Boca, C. Cobeli and A. Zaharescu, 'Distribution of lattice points visible from the origin', *Comm. Math. Phys.*, **213** (2000), 433–470.

[3] C. Cobeli and A. Zaharescu, 'On the distribution of the $\mathbb{F}_p$-points on an affine curve in r dimensions', *Acta Arithmetica*, **99** (2001), 321–329.

[4] A. Granville, I. E. Shparlinski and A. Zaharescu, 'On the distribution of rational functions along a curve over $\mathbb{F}_p$ and residue races', *J. Number Theory*, **112** (2005), 216–237.

[5] G. H. Hardy and E. M. Wright, *An Introduction to the theory of numbers*, The Clarendon Press, Oxford University Press, New York, 1979.

[6] M. N. Huxley and W. G. Nowak,'Primitive lattice points in convex planar domains', *Acta Arith.*, **76** (1996), 271–283.

[7] W. G. Nowak, 'Primitive lattice points inside an ellipse', *Czechoslovak Math. J.*, **55** (2005), 519–530.

[8] I. E. Shparlinski, 'Primitive points on a modular hyperbola', *Bull. Polish Acad. Sci. Math.*, **54** (2006), 193–200.

[9] M. Vajaitu and A. Zaharescu, 'Distribution of values of rational maps on the $\mathbb{F}_p$-points on an affine curve', *Monathsh. Math*, **136** (2002), 81–86.

[10] W. Zhai, 'On primitive lattice points in planar domains', *Acta Arith.*, **109** (2003), 1–26.

[11] Z. Zheng, 'The distribution of zeros of an irreducible curve over a finite field', *J. Number Theory*, **59** (1996), 106–118.