BULLETIN OF THE POLISH
ACADEMY OF SCIENCES
MATHEMATICS
Vol. 55, No. 3, 2007

NUMBER THEORY

Visible Points on Curves over Finite Fields

by

Igor E. SHPARLINSKI and José Felipe VOLOCH

Presented by Andrzej SCHINZEL

Summary. For a prime p and an absolutely irreducible modulo p polynomial $f(U,V) \in \mathbb{Z}[U,V]$ we obtain an asymptotic formula for the number of solutions to the congruence $f(x,y) \equiv a \pmod{p}$ in positive integers $x \le X$, $y \le Y$, 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 $1 \le X, Y \le p$ 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 is the set of points on level curves of $f(U,V)$ modulo p.

If $f(x,y) - a$ is a nonconstant absolutely irreducible polynomial modulo p of degree at least 2, then one can easily derive from the Bombieri bound [2] that

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

where the implied constant depends only on $\deg f$ (see, e.g., [3, 4, 9, 11]).

In this paper we consider an apparently new question of studying the cardinality of 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 $\mathcal{F}_{p,a}(X,Y)$

2000 *Mathematics Subject Classification*: 11A07, 11K38, 11L40.

Key words and phrases: points visible from the origin, absolutely irreducible polynomial.

which are "visible" from the origin (see [1, 6, 7, 10] and references therein for several other aspects of distribution of visible points in various regions).

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

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

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.

Our approach is based on a rather straightforward application of the inclusion-exclusion formula involving the Möbius function. We apply (1) to the lower terms of this formula which leads to the main term. However, the main difficulty is in getting a nontrivial estimate for the tail terms. This is exactly where we need to introduce some averaging in order to get such a nontrivial bound.

We recall $A \ll B$ and $A = O(B)$ both mean that $|A| \le cB$ 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

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

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 absolute 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 greater than one modulo the prime p.*

Then for real X and Y with $1 \le X, Y \le p$ 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 $a \in \{0, \dots, p-1\}$ 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 $d \ge 2$ is not square-free and $\mu(d) = (-1)^{\omega(d)}$ otherwise, where $\omega(d)$ is the number of distinct prime divisors of d. By the inclusion-exclusion principle, we write

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

Writing

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

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 $1 \le d < p$ then $f(dU, dV) - a$ remains absolutely irreducible modulo p. Accordingly, we have an analogue of (1) which asserts that

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

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

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

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

Furthermore

$$\sum_{d \le D} \frac{\mu(d)}{d^2} = \sum_{d=1}^{\infty} \frac{\mu(d)}{d^2} + O(D^{-1}) = \prod_l \left(1 - \frac{1}{l^2} \right) + O(D^{-1}),$$

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

$$\prod_l \left(1 - \frac{1}{l^2}\right) = \zeta(2)^{-1} = \frac{6}{\pi^2}$$

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

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

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

We also remark that

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

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

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

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. ∎

COROLLARY 3. *Let f be a polynomial with integer coefficients which is absolutely irreducible and of degree greater than one modulo the prime p. If $XY \ge p^{3/2}(\log p)^{2+\varepsilon}$ 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

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

We only consider polynomials f with integer coefficients such that the equation $f(x,y)=0$ has only finitely many integer solutions. We recall that the Siegel theorem guarantees this for a very general class of polynomials.

THEOREM 4. *Let f be a polynomial with integer coefficients which is absolutely irreducible and of degree greater than one such that the equation $f(x,y)=0$ has only finitely many integer solutions. Then for real T, X and Y such that $T \ge 2\max(X,Y)$ and $XY \ge T^{3/2}\log T$ we have*

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

as $T\to\infty$, where the sum is taken over all primes p with $T/2\le p\le T$.

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

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

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

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

Let $\mathcal{Z}$ be the set of integer zeros (x,y) of $f(x,y)=0$. We assume that D is large enough so that

$$f(ds,dt)\ne 0 \tag{11}$$

for $d>D$ and $s,t\ge 1$.

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 $\omega(|f(ds,dt)|)\ll\log(XY)\ll\log T$. Therefore

$$\begin{aligned}\sum_{T/2\le p\le T}\sum_{d>D}M_p(d;X,Y) &\le \sum_{d>D}\sum_{\substack{1\le s\le X/d\\ 1\le t\le Y/d}}\sum_{p\mid f(ds,dt)}1\\ &\le \sum_{d>D}\sum_{\substack{1\le s\le X/d\\ 1\le t\le Y/d}}\log T \ll XYD^{-1}\log T.\end{aligned}$$

We also note that by the prime number theorem,

$$\sum_{T/2 \le p \le T} \frac{1}{p} \le \frac{2}{T} \sum_{T/2 \le p \le T} 1 \ll \frac{1}{\log T}.$$

We now put everything together getting

$$\sum_{T/2 \le p \le T} \left| N_p(X,Y) - \frac{6}{\pi^2} \cdot \frac{XY}{p} \right| \ll \frac{XY}{D \log T} + DT^{3/2}(\log T)^2 + \frac{XY \log T}{D}$$
$$\ll DT^{3/2}(\log T)^2 + \frac{XY \log T}{D}.$$

We now take $D = cX^{1/2}Y^{1/2}T^{-3/4}(\log T)^{-1/2}$ for a sufficiently large constant c depending only on f (to guarantee that we have (11) for $d > D$ and $s, t \ge 1$), which yields the result. ∎

Corollary 5. *Let f be a polynomial with integer coefficients which is absolutely irreducible and of degree greater than one such that the equation $f(x,y) = 0$ has only finitely many integer solutions. If $T \ge 2\max(X,Y)$ and $XY \ge T^{3/2+\varepsilon}$ for some fixed $\varepsilon > 0$, then*

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

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

5. Remarks. Certainly it is interesting to obtain an asymptotic formula for $N_{p,a}(X,Y)$ which holds for every a. Even the case of $X = Y = p$ is of interest. We remark that for the polynomial $f(U,V) = UV$ such an asymptotic formula is given in [8] and is nontrivial provided $XY \ge p^{3/2+\varepsilon}$ 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 on the 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 than 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] F. P. Boca, C. Cobeli and A. Zaharescu, *Distribution of lattice points visible from the origin*, Comm. Math. Phys. 213 (2000), 433–470.

[2] E. Bombieri, *On exponential sums in finite fields*, Amer. J. Math. 88 (1966), 71–105.
[3] C. Cobeli and A. Zaharescu, *On the distribution of the $\mathbb{F}_p$-points on an affine curve in r dimensions*, Acta Arith. 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 Univ. 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*, Monatsh. Math. 136 (2002), 81–86.
[10] W. G. Zhai, *On primitive lattice points in planar domains*, Acta Arith. 109 (2003), 1–26.
[11] Z. Y. Zheng, *The distribution of zeros of an irreducible curve over a finite field*, J. Number Theory 59 (1996), 106–118.

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

José Felipe Voloch
Department of Mathematics
University of Texas
Austin, TX 78712, U.S.A.
E-mail: voloch@math.utexas.edu

Received May 14, 2007;
received in final form June 7, 2007 (7598)