ROCKY MOUNTAIN
JOURNAL OF MATHEMATICS
Volume 15, Number 2, Spring 1985

THE DISTRIBUTION OF RATIONAL POINTS ON A CURVE DEFINED MODULO Q

R. A. SMITH

1. Introduction. Let f be a polynomial defined over $\mathbf{Z}$ in two variables of total degree $d \geqq 2$, and let $V_p = \{\mathbf{x} \in C_p : f(\mathbf{x}) \equiv 0 \bmod p\}$ for each prime p, where $C_p = \{(x, y) \in \mathbf{Z}^2 : 0 \leqq x, y < p\}$. For each subset B in C_p, let $N_p(B) = \text{card}\,(B \cap V_p)$ and $N_p = \text{card}\, V_p$. If B is a box in C_p, that is,

$$B = \{(x,y) \in C_p : h < x \leqq h + H, k < y \leqq k + K\},$$

where $0 \leqq h < h + H \leqq p$ and $0 \leqq k < k + K \leqq p$, it is known that (cf. [2], [12])

$$\left| N_p(B) - \frac{|B|}{|C_p|} N_p \right| \leqq 4 \ln^2 p \max_{\mathbf{u} \in C_p^*} |S_p(\mathbf{u})|, \tag{1}$$

where $C_p^* = C_p - \{\mathbf{0}\}$ and $S_p(\mathbf{u})$ is the exponential sum defined by

$$S_p(\mathbf{u}) = \sum_{\mathbf{x} \in V_p} e_p(\mathbf{u} \cdot \mathbf{x}), \tag{2}$$

with $e_p(t) = \exp(2\pi i t/p)$. For simplicity, we shall assume that f is absolutely irreducible modulo p for all sufficiently large p, and so, by Weil's well-known result [14],

$$N_p = p + 0(p^{1/2}). \tag{3}$$

Furthermore, we know, by Bombieri [1] (or Chalk and Smith [4]), that

$$|S_p(\mathbf{u})| \leqq (d^2 + 2d - 3)p^{1/2} + d^2 \tag{4}$$

for each $\mathbf{u} \in C_p^*$. If we substitute these results into (1), we obtain

$$N_p(B) = \frac{|B|}{p} + O(p^{1/2} \ln^2 p), \tag{5}$$

for all sufficiently large p. (All O-terms are independent of p, though the inherent constant depends upon d; the same holds for the Vinogradov symbols $\ll$ and $\gg$.) This result shows that the zeros of $f(x,y)$ modulo p

Received by the editors July 4, 1983. . .

are uniformly distributed among boxes B in C_p for large p, provided that the cardinality of B is $\gg p^{3/2} \log^2 p$.

The purpose of this paper is to show that if certain incomplete exponential sums related to (2) satisfy their "expected" bounds, then (i) the measure of uniformity of the distribution of the points of V_p in C_p, as given by (5), can be substantially improved (cf., Theorem 1); and (ii) that the range of uniformity of certain asymptotic expansions in analytic number theory can be extended over what is presently known (cf., Theorems 2 and 3).

The idea of using incomplete exponential sums to study certain questions in number theory can already be found in Estermann's 1931 paper [5]. Recently, Iwaniec [9] pointed out that Hooley's Hypothesis R, (cf., [6, p. 75] and (11)) for incomplete Ramanujan sums leads to smaller solutions of the quadratic congruence $X^2 + Y^2 \equiv a \bmod p$, $(a, p) = 1$, than can be obtained from (5) alone (cf., Theorem 3). (This suggestion motivated our study of the more general question and led to Theorem 1.) Iwaniec's main idea is that by integrating the sum

$$\sum_{\substack{n \leq x \\ n \equiv a \bmod q}} a_n \tag{6}$$

over an interval against the invariant measure dz/z on $\mathbf{R}^+$, for certain arithmetic functions $\{a_n\}$, can lead to a very attractive formulation of the error term of (6) in terms of incomplete Ramanujan sums. In the case of the divisor function $d(n)$ and the circle function $r(n)$, we know that the asymptotic expansions of both

$$D(x; a, q) = \sum_{\substack{n \leq x \\ n \equiv a \bmod q}} d(n) \tag{7}$$

and

$$R(x; a, q) = \sum_{\substack{n \leq x \\ n \equiv a \bmod q}} r(n)$$

involve Kloosterman sums when q is not fixed. It is somewhat surprising that by smoothing both (7) and (8) analytically against the invariant measure dz/z leads to a corresponding "arithmetic smoothing" which certainly does not happen if we integrate against the non-invariant measure dz. As a result of this arithmetic smoothing, by which we mean that the error term in the asymptotic expansions of (7) and (8) can be expressed in terms of incomplete Ramanujan sums rather than complete Kloosterman sums, it follows that if Hypothesis R is correct, the range of uniformity in q of the asymptotic expansions of these sums can be extended all the way up to $X^{(3/4)-\varepsilon}$ rather than only up to $X^{2/3}$, which is the best we can presently do unconditionally (cf. Hooley [6] and Smith [11]).

2. Statement of results. Our first result depends upon the following hypothesis for each polynomial f in two variables over $\mathbf{Z}$ which is absolutely irreducible modulo p for all sufficiently large primes p.

HYPOTHESIS E_f. For each prime p, the incomplete exponential sum (cf., (2))

$$S_p(B^*; a) = \sum_{\substack{h<x\leqq h+H \\ 0<y\leqq p \\ f(x,y)\equiv 0 \pmod p}} e_p(ay),$$

where B^* is the 'vertical strip' defined by

$$B^* = \{(x, y) \in \mathbf{Z}^2 : h < x \leqq h + H, 0 < y \leqq p\}$$

satisfies

$$S_p(B^*; a) \ll H^{1/2}, \tag{9}$$

for all integers a, h and H with $(a, p) = 1$ and $p^{(1/2)+\varepsilon} < H < p$. (To avoid possible confusion, we are assuming that the constant inherent in $\ll$ is independent of a, h, H and p.)

We will now show that Hypothesis E_f is true on average. For, we clearly have

$$\sum_{0<a\leqq p} \Big| \sum_{\substack{h<x\leqq h+H \\ 0\leqq y\leqq p \\ f(x,y)\equiv 0 \bmod p}} e_p(ay)\Big|^2 = p \sum_{\substack{h<x\leqq h+H \\ 0\leqq y\leqq p \\ f(x,y)\equiv 0 \bmod p}} \sum_{\substack{h<x'\leqq h+H \\ f(x',y)\equiv 0 \bmod p}} 1 \tag{10}$$

$$\leqq dp\, N_p(B^*). \tag{11}$$

Moreover, the inner sum on the right hand side of (10) is $\leqq d$ since, for each $y = 1, 2, \ldots, p$, $f(X,Y)$ cannot vanish identically modulo p as a polynomial in X if p is large enough and $f(X,Y)$ is irreducible modulo p. This verifies the inequality in (11). In order to determine a respectable upper bound for $N_p(B^*)$, we appeal to the following well-known result (cf. Vinogradov [**13**, chap. V, exercise 12(*a*)]).

LEMMA 1. *If F is a complex valued function defined on the residue classes modulo p, then*

$$\Big|\sum_{h<x\leqq h+H} F(x) - \frac{H}{p}\sum_{0<x\leqq p} F(x)\Big| \leqq 2 \ln p \max_{1\leqq a<p}\Big|\sum_{0<x\leqq p} F(x)e_p(ax)\Big|.$$

In the application of this lemma, we take $\mathbf{u} = (0, a)$ in (2) and

$$F(x) = \sum_{\substack{0<y\leqq p \\ f(x,y)\equiv 0 \bmod p}} 1,$$

from which we deduce

$$\Big|N_p(B^*) - \frac{H}{p} N_p\Big| \leqq 2 \ln p \max_{1\leqq a<p} |S_p(\mathbf{u})|.$$

Hence, by (3) and (4), we immediately obtain

$$N_p(B^*) = H + O(p^{1/2} \ln p) \ll H, \tag{12}$$

if $H > p^{(1/2)+\varepsilon}$. Combining this result with (11) therefore implies that Hypothesis E_f is true on average, as asserted. (Moreover, this argument even proves that there exists at least one integer a with $(a, p) = 1$ satisfying (9)!)

If we now take $f(X, Y) = XY - 1$ in (9), which clearly is absolutely irreducible modulo p for all p, it is easily seen that Hypothesis E_f (for this special choice of f) is "essentially" identical with Hooley's Hypothesis R, when $q = p$ (a stronger version is given in [**8**, p. 44]):

HYPOTHESIS R. For all positive integers q the incomplete Ramanujan sum satisfies

$$\sum_{h<x\leq h+H} e_q(a\bar{x}) \ll H^{(1/2)+\varepsilon}(a, q)^{1/2},$$

whenever $q^{1/4} < H < q$.

Here, of course, the presence of an ε in the exponent on H is to account for the divisors of q.

THEOREM 1. *Let f be a non-linear polynomial in two variables over* $\mathbf{Z}$ *such that it is absolutely irreducible modulo p for all sufficiently large primes p. If B is any box in C_p with diameter $d(B) \geqq p^{(1/2)+\varepsilon}$, for any $\varepsilon > 0$, then Hypothesis E_f implies that*

$$N_p(B) = \frac{|B|}{p} + O(\sqrt{d(B)} \ln p).$$

An immediate consequence of this result is

COROLLARY 1. *Hypothesis E_f implies that every square box B with $|B| \gg p^{4/3} \ln p$ contains a point of V_p for all sufficiently large p. In particular, Hypothesis E_f implies that there exists integers $x, y \in \mathbf{Z}$ with* $\max(|x|, |y|) \ll p^{2/3} \ln p$ *satisfying $f(x, y) \equiv 0 \bmod p$, for all sufficiently large p.*

To illustrate this result, if $f(X, Y) = XY - a$ and $q = p$, then Hypothesis E_f and Hypothesis R are essentially equivalent, and imply that there exist integers x and y with $\max(|x|, |y|) \ll p^{(2/3)+\varepsilon}$ which satisfy $xy \equiv a \bmod p$ for any sufficiently large prime p with $(a, p) = 1$. As a second example, if $f(X, Y) = X^2 + Y^2 - a$, then Hypothesis E_f implies that there exist integers x and y with $\max(|x|, |y|) \ll p^{(2/3)+\varepsilon}$ which satisfy $x^2 + y^2 \equiv a \bmod p$. What is rather surprising is that this also follows from Hypothesis R (cf., Corollary 2), even though Hypothesis E_f and R are apparently unrelated.

THEOREM 2. *If a and q are relatively prime integers with q positive, then Hypothesis R implies that*

$$\sum_{\substack{n \leqq X \\ n \equiv a \bmod q}} d(n) \ln \frac{X}{n}$$
$$= \frac{\phi(q)}{q^2}\left(X \ln X + 2\left(\gamma - 1 - q\frac{\phi'(q)}{\phi(q)}\right)X\right) + O\left(X^{(1/4)+\varepsilon} + q^{-1}X^{(1/2)+\varepsilon}\right)$$

as $X \to \infty$, where γ is Euler's constant, ϕ is the Euler phi-function and $\phi'(q) = \sum_{d|q}(\mu(d)/d)\ln d$. Moreover, this asymptotic expansion holds uniformly in $q \leqq X^{(3/4)-\varepsilon}$, for any fixed $\varepsilon > 0$.

THEOREM 3. *If a and q are relatively prime integers with q positive, then Hypothesis R implies that*

$$\sum_{\substack{n \leqq X \\ n \equiv a \bmod q}} r(n) \ln \frac{X}{n} = \frac{\pi X}{q} \prod_{p|q}\left(1 - \frac{\chi_4(p)}{p}\right) + (X^{(1/4)+\varepsilon} + q^{-1}X^{(1/2)+\varepsilon})$$

as $X \to \infty$ where χ_4 is the non-principal character modulo 4. Moreover, this asymptotic expansion holds uniformly in $q \leqq X^{(3/4)-\varepsilon}$, for any fixed $\varepsilon > 0$.

COROLLARY 2. *If a and q are relatively prime integers with q positive, then Hypothesis R implies that there exist integers x and y with $\max(|x|, |y|) \ll q^{(2/3)+\varepsilon}$ such that $x^2 + y^2 \equiv a \bmod q$.*

By a standard unsmoothing argument, Theorems 2 and 3 lead to corresponding results for these sums without the weighting factor $\ln(X/n)$. Moreover, because the proofs of Theorems 2 and 3 are so similar, we will only prove the former, which is slightly simpler to handle.

Finally, the result of Corollary 2 suggests that we should look for a similar result for Corollary 1. Indeed, this can be done by a straight-forward extension of Hypothesis E_f for square-free q, since the "expected" bound for the corresponding incomplete exponential sum can be obtained as in (11). On the other hand, if q is arbitrary, we do not have a good upper bound for N_q (except, for example, when f has no singular zeros in the finite field $\mathbf{F}_p$, for each $p|q$; cf., Chalk [3], p. 58) and so we cannot yet anticipate what the "expected" size of such incomplete exponential sums should be. Moreover, if we had an analogue of Theorem 2 in [10] of Loxton and Smith for polynomials in *two* variables, we could then formulate Hypothesis E_f quite generally for arbitrary q and arbitrary polynomials f containing no linear factors. Such a result would perhaps lead to a further generalization of Theorem 1, though it is by no means certain. The first step in this direction would be to obtain an analogue of Corollary 2 for $f(X, Y) = XY - a$, without recourse to Hypothesis R.

3. Proof of Theorem 1. If the sums over x in Lemma 1 are replaced by their corresponding sums over y, and if we take

$$F(y) = \sum_{\substack{h<x\leqq h+H \\ f(x,y)\equiv 0 \bmod p}} 1,$$

we then obtain

$$\left|N_p(B) - \frac{K}{p}N_p(B^*)\right| \leqq 2 \ln p \max_{1\leqq a\leqq p} |S_p(B^*, a)|,$$

where $S_p(B^*; a)$ is the incomplete exponential sum defined in (9). If we now assume that Hypothesis E_f holds, and if we apply the result in (12), we then obtain

$$N_p(B) = \frac{|B|}{p} + O((H^{1/2} + p^{-1/2}K)\ln p). \tag{13}$$

Moreover, if we perform the summation in deriving (13) in the other order, we would then obtain

$$N_p(B) = \frac{|B|}{p} + O((K^{1/2} + p^{-1/2}H)\ln p),$$

and this, or (13), implies that

$$N_p(B) = \frac{|B|}{p} + O(\max(H, K)^{1/2}\ln p)$$

from which the theorem follows.

4. Proof of Theorem 2. By a standard geometrical argument, together with elementary arithmetic considerations, we have

$$D(z; a, q) = 2 \sum_{\nu\leqq z^{1/2}}^{*} \sum_{\substack{\lambda\leqq z/\nu \\ \lambda\equiv a\bar{\nu} \bmod q}} 1 - \sum_{\nu\leqq z^{1/2}}^{*} \sum_{\substack{\lambda\leqq z^{1/2} \\ \lambda\equiv a\bar{\nu} \bmod q}} 1, \tag{14}$$

where $\sum_p^*$ means that we sum only over those ν's that are relatively prime to q, and for each such ν, we define $\bar{\nu}$ by $\nu\bar{\nu} \equiv 1 \bmod q$. For any $0 < \nu \leqq X^{1/2}$ and relatively prime to q, and for any $0 < U \leqq X/\nu$, we have

$$\sum_{\substack{\lambda\leqq U \\ \lambda\equiv a\bar{\nu} \bmod q}} 1 = \left[\frac{U - a\bar{\nu}}{q}\right] - \left[\frac{-a\bar{\nu}}{q}\right] = \frac{U}{q} = \left(\psi\left(\frac{U-a\bar{\nu}}{q}\right) - \psi\left(\frac{-a\bar{\nu}}{q}\right)\right), \tag{15}$$

where $\psi(x) = x - [x] - (1/2)$, $[x]$ denoting the largest integer $\leqq x$. Consequently, the main contribution in the asymptotic expansion of

$$\sum_{\substack{n\leqq X \\ n\equiv a \bmod q}} d(n)\ln\frac{X}{n} \int_1^X = D(z; a, q)\frac{dz}{z}, \tag{16}$$

as $X \to \infty$, is given by

$$\frac{1}{q}\int_1^X \sum_{\nu\le z^{1/2}}^{*}\left(\frac{2z}{\nu}-z^{1/2}\right)\frac{dz}{z}$$
$$=\frac{1}{q}\sum_{d\mid q}\mu(d)\int_1^X\left(\frac{2}{d}\sum_{\nu\le z^{1/2}/d}\frac{1}{\nu}-z^{-1/2}[z^{1/2}/d]\right)dz$$
$$=\frac{\phi(q)}{q^2}\left(X\ln X+2\left(\gamma-1-q\frac{\phi'(q)}{\phi(q)}X\right)\right)+O(q^{-1}X^{1/2}),$$

after some routine calculations.

In view of (14) and (15), the remaining terms in the expansion of (16) are given by

$$\int_1^X \sum_{\nu\le z^{1/2}}^{*}\left\{-2\psi\left(\frac{z/\nu-a\bar{\nu}}{q}\right)+\psi\left(\frac{z^2-a\bar{\nu}}{q}\right)+\psi\left(\frac{-a\bar{\nu}}{q}\right)\right\}\frac{dz}{z}=-2S_1+S_2+S_3,$$

respectively, say. In S_1, we interchange the order of summation and integeration to obtain

$$S_1=\sum_{\nu\le X^{1/2}}^{*}\int_{\nu^2}^{X}\psi\left(\frac{z/\nu-a\bar{\nu}}{q}\right)\frac{dz}{z}.$$

If we replace the integration variable z by νz, and observe that the dz/z is invariant under this change of variable, we then obtain

$$S_1=\sum_{\nu\le X^{1/2}}^{*}\int_{\nu}^{X/\nu}\psi\left(\frac{z-a\bar{\nu}}{q}\right)\frac{dz}{z}.$$

Finally, we change the order of summation and integration once again to obtain

$$S_1=\int_1^X \sum_{\nu\le \min(z,\,X/z)}^{*}\psi\left(\frac{z-a\bar{\nu}}{q}\right)\frac{dz}{z}.$$

Thus, all three integrals S_i are of the form

$$\int_1^X \sum_{\nu\le U(z)}^{*}\psi\left(\frac{V(z)-a\bar{\nu}}{q}\right)\frac{dz}{z},$$

where $U=U(z)$ and $V=V(z)$ are non-negative continuous functions of z with $1\le z\le X$, and where $V(z)$ is independent of ν. In order to bound the integrals in (18), we now use Estermann's Fourier expansion of ψ given in [**5**, Hilfsatz 3].

LEMMA 2. *For any $0<\Delta<1/4$, there exists a pair of Fourier series A and B such that for all x,*

$$|\psi(x)-A(x)|\le 9\Delta+B(x),$$

where

$$A(x)=\frac{1}{2\pi i}\sum_{0<|n|\le\Delta^{-2}}\frac{1}{n}e^{2\pi inx}$$

and

$$B(x) = \sum_{n \neq 0} b_n e^{2\pi i n x}$$

with

$$0 \leqq b_n \leqq 2 \min\left(\frac{1}{|n|}, \frac{1}{\Delta n^2}\right),$$

for $n \neq 0$.

Thus, Lemma 2 implies that

$$\left|\int_1^X \sideset{}{^*}\sum_{\nu \leqq U(z)} \psi\left(\frac{V(z) - a\bar{\nu}}{q}\right)\frac{dz}{z}\right| \leqq 9\Delta\int_1^X U(z)\frac{dz}{z} + \int_1^X \sideset{}{^*}\sum_{\nu \leqq U(z)} B\left(\frac{V(z) - a\bar{\nu}}{q}\right)\frac{dz}{z} + \left|\int_1^X \sideset{}{^*}\sum_{\nu \leqq U(z)} A\left(\frac{V(z) - a\bar{\nu}}{q}\right)\frac{dz}{z}\right|, \tag{17}$$

from which it is clear that in order to bound the last two integrals in (17), it suffices to examine

$$\int_1^X \left|\sideset{}{^*}\sum_{\nu \leqq U(z)} e_q(-an\bar{\nu})\right|\frac{dz}{z}. \tag{18}$$

By chopping up the sum in (18) into pieces of length q, plus an extra bit at the end, we find that (18) is

$$\leqq q^{-1}|c_q(n)|\int_1^X U(z)\frac{dz}{z} + \int_1^X \left|\sum_{\nu \in I(q,z)} e_q(-an\bar{\nu})\right|\frac{dz}{z}, \tag{19}$$

where $c_q(n)$ is the Ramanujan sum and $I(q, z)$ is the interval of length $< q$ defined by

$$I(q, z) = \{x: q[q^{-1}[U(z)]] < x \leqq U(z)\}.$$

Since $U(z)$ is either $z^{1/2}$ or $\min(z, X/z)$ in the application, the first term in (19) is

$$\ll q^{-1}|c_q(n)|X^{1/2}.$$

Finally, we are left with the second term in (19), which involves incomplete Ramanujan sums over ranges of length $< q$. The contribution to this term from the set of $z \in [1, X]$, for which $|I(q, z)| \leqq q^{1/4}$, is trivially

$$\ll \int_1^X q^{1/4}\frac{dz}{z} \ll q^{\varepsilon}X^{1/4},$$

since we may assume $q \leqq X$ without loss of generality. For the remaining part of the integral, we apply Hypothesis R and find that the contribution is

$$\ll (n,q)^{1/2}q^{\varepsilon}\int_1^X |I(q,z)|^{1/2}\frac{dz}{z} \ll (n,q)^{1/2}\, q^{\varepsilon}\int_1^X U(z)^{1/2}\frac{dz}{z} \ll (n,q)^{1/2}q^{\varepsilon}X^{1/4}.$$

Combining these results, we find that

$$\int_1^X \Big|\sum_{\nu \bmod U(z)}^{*} e_q(-\mathrm{an}\bar{\nu})\Big|\frac{dz}{z} \ll q^{-1}|c_q(n)|X^{1/2} + (n,q)^{1/2}q^{\varepsilon}X^{1/4},$$

whence (17) implies

$$\int_1^X \sum_{\nu \bmod U(z)}^{*} \psi\Big(\frac{V(z) - a\bar{\nu}}{q}\Big)\frac{dz}{z} \ll (q^{-1}X^{1/2} + X^{1/4})q^{\varepsilon}$$

if we pick $\Delta = (4q)^{-1}$. This completes the proof.

References

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

2. J. H. H. Chalk, *The number of solutions of congruences in incomplete residue systems*, Canadian J. Math. **15** (1963), 291–296.

3. ———, *Incomplete residue systems to a composite modulus*, C. R. Math. Rep. Acad. Sci. Canada **5** (1983), 55–60.

4. ———, and R. A. Smith, *On Bombieri's estimate for exponential sums*, Acta Arith. **18** (1971), 191–212.

5. T. Estermann, *Über die Darstellungen einer Zahl als Differenz von zwei Produkten*, J. reine angew. Math. **164** (1931), 173–182.

6. C. Hooley, *An asymptotic formula in the theory of numbers*, Proc. Lond. Math. Soc. (3) **7** (1957), 396–413.

7. ———, *On the Brun-Titchmarsh theorem*, J. reine angew. Math. **255** (1972), 60–82.

8. ———, *Greatest prime factor of a cubic polynomial*, J. reine angew. Math. **303/304** (1978), 21–50.

9. H. Iwaniec, letter to J. H. H. Chalk (1979).

10. J. H. Loxton and R. A. Smith, *On Hua's estimates for exponential sums*, J. Lond. Math. Soc. (2) **26** (1982), 15–20.

11. R. A. Smith, *The circle problem in an arithmetic progression*, Canadian Math. Bull. **11** (1968), 175–184.

12. ———, *The distribution of rational points on hypersurfaces defined over a finite field*, Mathematika **17** (1970), 328–332.

13. I. M. Vinogradov, *Elements of Number Theory*, Dover, 1954.

14. A. Weil, *On the Riemann Hypothesis for function fields*, Proc. Nat. Acad. Sci., U.S.A. **27** (1941), 345–347.

Department of Mathematics, University of Toronto, Toronto Canada M5S 1A1

Prof. R. A. Smith died on March 30, 1983.