

COUNTING POINTS MODULO p FOR SOME FINITELY GENERATED SUBGROUPS OF ALGEBRAIC GROUPS

C. R. MATTHEWS

0. Introduction

We begin by explaining the basic idea of this paper in a simple case. We write n_p for the order of 2 modulo the prime p , so that n_p is the number of powers of 2 which are distinct mod p . We have the elementary bounds

$$\log p \ll n_p \leq p-1.$$

The conjecture of E. Artin on primitive roots asserts that the upper bound is attained for a set of primes with positive density (see Hooley [2] for a discussion of conditional proofs in this case). The lower bound may be improved to

$$p^{\frac{1}{2}-\varepsilon} < n_p$$

for almost all primes p , in the sense of density, for any $\varepsilon > 0$. To see this, let $E(x)$ count the primes less than x for which this estimate fails. Given any such prime p , there is r with

$$1 \leq r \leq p^{\frac{1}{2}-\varepsilon}$$

such that p divides $2^r - 1$. A form of the "box principle" implies that there is some m with

$$1 \leq m \leq x^{\frac{1}{2}-\varepsilon}$$

and such that $2^m - 1$ is divisible by at least the average number

$$E(x)/x^{\frac{1}{2}-\varepsilon}$$

of such primes. The standard estimate

$$\omega(n) \ll \log n / \log \log n$$

for the number $\omega(n)$ of distinct prime divisors of n then gives

$$E(x)/x^{\frac{1}{2}-\varepsilon} \ll m / \log m \ll x^{\frac{1}{2}-\varepsilon} / \log x$$

which shows

$$E(x) = o(x / \log x)$$

as required.

Received 30 July, 1981; revised 26 August, 1981.

Bull. London Math. Soc., 14 (1982), 149–154.

It should be clear that this argument may be adapted to estimate the size of exceptional sets for other lower bounds. For example, one may prove in this way that for any positive δ we may find $C(\delta)$ such that n_p is at least $C(\delta)p^\delta$ for all but $\delta x/\log x$ primes less than x . To get sharper results by this method we would need better estimates for

$$\sum_{m \leq x} \omega(2^m - 1)$$

than follow from estimating each term separately.

The object of this paper is to establish lower bounds of the kind given above, for a broad range of questions in the direction of Artin's conjecture. For a survey of many of the variants which have been considered, the reader may consult the paper [3] of Lenstra. From our point of view some general formulations in terms of algebraic groups are suggested; the results we obtain apply to affine algebraic groups or abelian varieties.

We suppose first that we are given a class of algebraic groups G defined over \mathbf{Q} , with reductions G_p defined over \mathbf{F}_p for sufficiently large primes p . For an abstract finitely generated group Γ we consider injective representations $\phi : \Gamma \rightarrow G(\mathbf{Q})$, and wish to give lower bounds for the size of $\phi(\Gamma)$ modulo p , in the following sense: for p large we may compose ϕ with reduction mod p to give a homomorphism

$$\rho_p : \Gamma \rightarrow G_p(\mathbf{F}_p),$$

and we write Γ_p for the image. Then given an increasing function F we have the problem

- I: Find upper bounds for $E(x) = |\{p \leq x : |\Gamma_p| < F(x)\}|$, valid for all injective representations ϕ in the class considered.

A more precise question is

- II: Given a particular choice of ϕ in I, find upper bounds for $E(x)$.

A natural formulation of the idea of the classical conjecture is

- III: Suppose given, in the context of II, a subgroup H of G , also defined over \mathbf{Q} , with reductions H_p for p large. Find upper bounds for $E_H(x) = |\{p \leq x : \Gamma_p \text{ does not contain } H_p(\mathbf{F}_p)\}|$.

To recover the classical case from III we take $G = H = \text{GL}_1$, and Γ an infinite cyclic subgroup of the multiplicative group of \mathbf{Q} .

Our method gives the results in the context of I, the essentially elementary nature of the argument not taking into account the finer structure of a representation.

When Γ is infinite cyclic there is no important case of these problems which is properly understood. It is worth noting therefore that this is not true for other groups; for example if Γ is $\text{SL}_2(\mathbf{Z})$, and ϕ the natural representation in $\text{SL}_2(\mathbf{Q})$, it is easy to see that Γ_p is $\text{SL}_2(\mathbf{F}_p)$ for all p .

We give further discussion of the case of abelian varieties in Section 2 below.

NOTATION. We write $|X|$ for the cardinality of a finite set X . If G is an algebraic group over a field K then $G(K)$ is the group of K -rational points of G . We use \mathbf{F}_p for the field with p elements. If f, g are positive functions we write $f \ll g$ if $f(x) \leq Cg(x)$ for x large and some constant C .

1. *Linear algebraic groups*

In this section we suppose given a finitely generated group Γ of rational $n \times n$ matrices. There are only finitely many primes p which divide the determinant of an element of Γ , or the denominator of an entry of an element of Γ . We exclude these primes; we may then define a reduction homomorphism $\rho_p: \Gamma \rightarrow \text{GL}_n(\mathbb{F}_p)$ in the natural way: we use entry by entry the reduction homomorphism $\mathbb{Z}_{(p)} \rightarrow \mathbb{F}_p$ of the local ring $\mathbb{Z}_{(p)}$ of rational numbers with denominators prime to p . We write $\Gamma^{(p)}$ for the kernel of ρ_p , and Γ_p for its image. An element of Γ other than the identity I lies in $\Gamma^{(p)}$ only for finitely many p ; we quantify this using suitable measures of the complexity of elements of Γ .

We first define the height of a rational non-zero matrix M as follows: write M as $d(M)^{-1}M'$ with $d(M)$ an integer and $M' = (m'_{ij})$ with integral m'_{ij} having no common factor. Then set

$$h(M) = \log \max (|d(M)|, |m'_{ij}|).$$

The crucial property of this height is the

LEMMA. *There exist a finite subset S of Γ and a constant C such that an element γ of Γ which does not lie in S belongs to $\Gamma^{(p)}$ for at most $Ch(\gamma)/\log h(\gamma)$ primes p .*

Proof. We write γ as $d(\gamma)^{-1}N$ as above. Then γ lies in $\Gamma^{(p)}$ only if $d(\gamma)I$ is congruent to $N \pmod p$. We assume that γ is not I , so that $d(\gamma)I - N$ has a non-zero entry a , say. The number of primes p with γ in $\Gamma^{(p)}$ is therefore bounded by $\omega(|a|)$, the number of prime factors of $|a|$. We have the classical estimate

$$\omega(n) \ll \log n / \log \log n$$

(already a consequence of the elementary estimates of prime number theory, cf. [1] Chapter XXII). Since we clearly have

$$\log |a| \leq 2h(\gamma),$$

this gives the required result.

We now suppose chosen a finite set \mathcal{A} of generators for Γ , such that $\mathcal{A}^{-1} = \mathcal{A}$. We define the length $l(\gamma)$ of an element to be the least integer l such that we may write γ as $\alpha_1 \dots \alpha_l$ with the α_i in \mathcal{A} ; we agree that $l(I)$ is 0.

It is easy to see that

$$h(\gamma_1 \gamma_2) \leq h(\gamma_1) + h(\gamma_2) + \log n.$$

It follows that we have $h(\gamma) \ll l(\gamma)$ with the implied constant depending on $\max \{h(\alpha) : \alpha \text{ in } \mathcal{A}\}$. This gives

COROLLARY. *There exist a finite subset S' of Γ and a constant C' such that an element γ of Γ which is not in S' lies in $\Gamma^{(p)}$ for at most $C'l(\gamma)/\log l(\gamma)$ primes p .*

We define the counting function $L(x)$ as $|\{\gamma \in \Gamma : l(\gamma) \leq x\}|$. This is the *rate of growth* of Γ , as studied by Milnor [4], [5] and others. We now formulate the idea of our method.

THEOREM 1. *Suppose given a positive function F which tends to infinity with x , and such that $F/\log F$ is increasing. Defining $E(x)$ as the number of primes less than x such that*

$$|\Gamma_p| < L(F(x)),$$

we have

$$E(x) \ll L(2F(x))F(x)/\log F(x).$$

Proof. In establishing the inequality, we may disregard any fixed finite set of primes; we choose to ignore p if ρ_p is not defined, or if there is some γ in the exceptional set S' above with γ not I and γ in $\Gamma^{(p)}$. Setting aside such primes, we suppose p such that $|\Gamma_p|$ is less than $L(F(x))$; then among the $L(F(x))$ elements of Γ of length at most $F(x)$, there will certainly be distinct γ_1, γ_2 with the same image in Γ_p under ρ_p . It follows that $\gamma_1\gamma_2^{-1}$ lies in $\Gamma^{(p)}$; call it $\gamma^{(p)}$. By assumption $\gamma^{(p)}$ is not I and is not in S' , and it clearly has length at most $2F(x)$.

If we choose an element $\gamma^{(p)}$ in this way for each of the primes in question, which are $E(x)$ in number, we have at most $L(2F(x))$ candidates from which to select; therefore some element γ is chosen in this way at least the average number $E(x)/L(2F(x))$ of times. By construction we may apply the Corollary above to give

$$E(x)/L(2F(x)) \ll l(\gamma)/\log l(\gamma).$$

Since γ has length at most $2F(x)$, our assumptions on F show that

$$l(\gamma)/\log l(\gamma) \ll F(x)/\log F(x),$$

so that the result follows.

A first application of this theorem is to the case of infinite cyclic Γ . Choosing \mathcal{A} to consist of a generator and its inverse, we have $L(x) = 2[x] + 1$. With $F(x)$ taken to be $x^{\frac{1}{2}-\epsilon}$ we find again the result given in the *Introduction*, in this broader context: we have

$$|\Gamma_p| > p^{\frac{1}{2}-\epsilon}$$

for almost all primes p (in the sense of density).

In general, results of Wolf [8] and Tits [7] show that one of two possibilities holds: the rate of growth $L(x)$ may lie between constant multiples of x^d for some integer d , or between constant multiples of e^{cx} for some positive c . The first of these occurs if and only if Γ has a nilpotent subgroup of finite index, and the integer d is determined by the structure of Γ ; for example when Γ is abelian, d is its rank. In this case we choose $F(x)$ to be $x^{1/(d+1)-\epsilon}$ for any positive ϵ , and find that for almost all p we have

$$|\Gamma_p| > p^{d/(d+1)-\epsilon}.$$

In the case of exponential growth we have $L(2F(x))$ of the order of $L(F(x))^2$, so that the estimates given by the theorem are no better than for an infinite cyclic subgroup. The typical case here is of Γ free on two generators. In the context of Problem I of the *Introduction* it is clear that we will not have estimates for free Γ which are improved for large rank (as non-abelian free groups contain free subgroups of larger rank), in contrast to what we have shown for abelian groups. It is an interesting

question therefore to ask if free groups on one and many generators are genuinely on a par, as our results suggest.

2. *Abelian varieties*

We will show that the use of the Tate–Néron height function permits a straightforward carrying-over to abelian varieties of the idea of the previous section. We shall suppose some familiarity on the part of the reader with the theory of heights (see for example the paper [6] of Néron) and of abelian varieties.

Suppose that A is an abelian variety defined over \mathbf{Q} , and that ϕ is a symmetric embedding of A in \mathbf{P}^n , also defined over \mathbf{Q} . The naïve height function associated to ϕ is defined as follows: for a rational point P of \mathbf{P}^n , represented in a fixed coordinate system by a set (X_0, \dots, X_n) of integral homogeneous coordinates without common factor, we define $h(P)$ to be $\log \max |X_i|$, and for Q in $A(\mathbf{Q})$ we define $h_\phi(Q)$ to be $h(\phi(Q))$. After Mordell and Weil we know that $A(\mathbf{Q})$ is a finitely generated abelian group; Tate and Néron showed that h_ϕ is approximately quadratic on $A(\mathbf{Q})$, in the sense that there exists a quadratic form \hat{h} on $A(\mathbf{Q})$ with $h_\phi - \hat{h}$ bounded. We have $\hat{h}(Q)$ non-negative and equal to zero only if Q is a torsion element of $A(\mathbf{Q})$.

For all sufficiently large primes p we have a reduced abelian variety A_p , defined over \mathbf{F}_p and embedded projectively by the reduction of ϕ ; there is a reduction map giving a homomorphism

$$\rho_p : A(\mathbf{Q}) \rightarrow A_p(\mathbf{F}_p)$$

of abelian groups.

LEMMA. *There exist a finite subset S of $A(\mathbf{Q})$ and a constant C such that if Q is an element of $A(\mathbf{Q})$ which is not in S , Q lies in the kernel of ρ_p for at most $C\hat{h}(Q)/\log \hat{h}(Q)$ primes p .*

Proof. The proof of the corresponding assertion for h_ϕ runs on the same lines as for the lemma of the previous section. Since $h_\phi - \hat{h}$ is bounded we may replace h_ϕ by \hat{h} , possibly at the cost of changing S and C .

Now suppose given a subgroup Γ of $A(\mathbf{Q})$, of rank r say. The rate of growth $L(x)$ of Γ , as defined before, lies between constant multiples of x^r , for any choice of generating set \mathcal{A} . The quadratic nature of $\hat{h}(Q)$ means that we have

$$\hat{h}(Q) \ll l(Q)^2$$

so as corollary of the lemma we have a constant multiple of

$$l(Q)^2 / \log l(Q)$$

as bound for the number of primes p with Q in $\ker \rho_p$, for Q outside some finite subset of $A(\mathbf{Q})$.

THEOREM 2. *Suppose that F is a positive function, tending to infinity with x , with $F^2/\log F$ increasing. If $E(x)$ is the number of primes less than x such that*

$$|\rho_p(\Gamma)| < F(x)^r,$$

we have

$$E(x) \ll F(x)^{r+2} / \log F(x).$$

Proof. Follow Theorem 1 with appropriate minor changes.

Choosing $x^{1/(r+2)-\varepsilon}$ for $F(x)$, for any positive ε , we find this time that $|\rho_p(\Gamma)|$ is almost always as large as $p^{r/(r+2)-\delta}$, any positive δ , in the sense of density.

When A is an elliptic curve we have $|A_p(\mathbb{F}_p)|$ of order p , so that the limiting value $r/(r+2) \rightarrow 1$ for large rank is the natural bound. It is of considerable interest to find bounds for A of higher dimension d which are closer to the asymptotic value p^d for $|A_p(\mathbb{F}_p)|$; it is conceivable that progress might lead to bounds on the rank of abelian varieties.

NOTE added in proof, October 1981: For the elliptic curve analogue of Artin's conjecture see S. Lang and H. Trotter, *Bull. Amer. Math. Soc.*, 83 (1977), 289–292.

ACKNOWLEDGMENT. The author is a Research Fellow at Christ's College, Cambridge.

References

1. G. H. HARDY and E. M. WRIGHT, *An introduction to the theory of numbers* (Oxford University Press, Oxford, 1979 (5th edition)).
2. C. HOOLEY, *Applications of sieve methods to the theory of numbers* (Cambridge University Press, Cambridge, 1976).
3. H. W. LENSTRA, 'On Artin's conjecture and Euclid's algorithm in global fields', *Invent. Math.* 42 (1977), 201–224.
4. J. MILNOR, 'A note on curvature and the fundamental group', *J. Differential Geom.* 2 (1968), 1–7.
5. J. MILNOR, 'Growth of finitely generated solvable groups', *J. Differential Geom.* 2 (1968), 447–449.
6. A. NÉRON, 'Quasi-fonctions et hauteurs sur les variétés abéliennes', *Ann. of Math.* 82 (1965), 249–331.
7. J. TITS, 'Free subgroups in linear groups', *J. Algebra* 20 (1972), 250–270.
8. J. A. WOLF, 'Growth of finitely generated solvable groups and curvature of Riemannian manifolds', *J. Differential Geom.* 2 (1968), 421–446.

Christ's College,
Cambridge.

