A LOCAL-GLOBAL PRINCIPLE FOR DENSITIES

BJORN POONEN AND MICHAEL STOLL

Abstract. This expository note describes a method for computing densities of subsets of $\mathbf{Z}^n$ described by infinitely many local conditions.

1. Introduction

The aim of this note is to present a general method for studying questions such as the following.

Fix $g \geq 1$. What is the 'probability' that a curve of the form

$$y^2 = f(x) = a_{2g+2}x^{2g+2} + a_{2g+1}x^{2g+1} + \cdots + a_2x^2 + a_1x + a_0 \tag{1}$$

with $a_j \in \mathbf{Z}$ has genus g and has $\mathbf{Q}_v$–rational points for all completions $\mathbf{Q}_v$ of $\mathbf{Q}$?

To make sense of this quesion, we have to make precise what we mean by 'probability.' We choose the coefficients a_j randomly from the integers of absolute value at most N and ask for the probability that the resulting curve has the property in question; then we take the limit of this as $N \to \infty$ and call the result a *density*.

Definition. For $v = (v_1, v_2, \ldots, v_d) \in \mathbf{Z}^d$, define $|v| := \max_i |v_i|$. If $S \subseteq \mathbf{Z}^d$, then the *density* of S is defined to be

$$\rho(S) := \lim_{N\to\infty} \frac{\#\{v \in S : |v| \leq N\}}{(2N+1)^d},$$

if the limit exists. Define the *upper density* $\overline{\rho}(S)$ and *lower density* $\underline{\rho}(S)$ similarly, except with the limit replaced by a lim sup or lim inf, respectively.

Note that in our question, the condition that (1) has genus g is equivalent to the nonvanishing of the discriminant $\Delta(a_0, a_1, \ldots, a_{2g+2})$ of f. We have chosen to exclude such curves for our density calculation, but this is of no consequence since the entire zero locus of Δ in $\mathbf{Z}^{2g+3}$ has density zero.

What makes our question difficult is that we are imposing conditions at infinitely many primes. If we wanted only an estimate for the density of curves (1) that had points over $\mathbf{R}$, $\mathbf{Q}_2$, and $\mathbf{Q}_{17}$, say, but required neither the existence nor the lack of points over the other $\mathbf{Q}_p$, then the question could easily be reduced to the computation of corresponding local probabilities, by invoking weak approximation to prove the 'independence' of the conditions being imposed.

We will show that our original question also can be reduced to the computation of local probabilities. Most of the proofs will be left out for reasons of space; they can be found in [PSt]. In that paper, the method is applied to prove results on the density of hyperelliptic

Date: February 26, 1998.

Much of this research was done while the first author was supported by an NSF Mathematical Sciences Postdoctoral Research Fellowship at Princeton University. This article has been published in *Topics in Number Theory*, S. D. Ahlgren et al. (eds.), Kluwer, 1999, 241–244.

curves whose Jacobians have a Shafarevich-Tate group of non-square order (if finite). But the method undoubtedly has many other interesting applications.

First we need some more notation. If S is a set, then 2^S denotes its power set. If K is a number field, let M_K denote the set of places of K. For example, $M_{\mathbf{Q}} = \{\infty\} \cup \{p : p \text{ prime}\}$. Finally, we let μ_∞ denote the standard Lebesgue measure on $\mathbf{R}^d$, and let μ_p denote the Haar measure on $\mathbf{Z}_p^d$ normalized to have total mass 1.

2. The results

We formalize the method for obtaining density results in the following lemma.

Lemma 1. *Suppose that U_∞ is a subset of $\mathbf{R}^d$ such that $\mathbf{R}^+ \cdot U_\infty = U_\infty$ and $\mu_\infty(\partial U_\infty) = 0$. Let $U_\infty^1 = U_\infty \cap [-1,1]^d$, and let $s_\infty = 2^{-d}\mu_\infty(U_\infty^1)$.*[1] *Suppose that for each finite prime p, U_p is a subset of $\mathbf{Z}_p^d$ such that $\mu_p(\partial U_p) = 0$. Let $s_p = \mu_p(U_p)$. Finally, suppose that*

$$\lim_{M\to\infty} \overline{\rho}\left(\left\{a \in \mathbf{Z}^d : a \in U_p \text{ for some finite prime } p \text{ greater than } M\right\}\right) = 0. \tag{2}$$

Define a map $P : \mathbf{Z}^d \longrightarrow 2^{M_{\mathbf{Q}}}$ as follows: if $a \in \mathbf{Z}^d$, let $P(a)$ be the set of places v such that $a \in U_v$. Then

1. *$\sum_v s_v$ converges.*
2. *For $\mathfrak{S} \subseteq 2^{M_{\mathbf{Q}}}$, $\nu(\mathfrak{S}) := \rho(P^{-1}(\mathfrak{S}))$ exists, and ν defines a measure on $2^{M_{\mathbf{Q}}}$.*
3. *The measure ν is concentrated at the finite subsets of $M_{\mathbf{Q}}$: for each finite subset S of $M_{\mathbf{Q}}$,*

$$\nu(\{S\}) = \prod_{v\in S} s_v \prod_{v\notin S}(1 - s_v), \tag{3}$$

and if $\mathfrak{S} \subset 2^{M_{\mathbf{Q}}}$ consists of infinite subsets of $M_{\mathbf{Q}}$, then $\nu(\mathfrak{S}) = 0$.

Proof. See [PSt, Lemma 20]. □

For our original question, we will eventually take $d = 2g + 3$ and let U_p (resp. U_∞) be the set of $(a_0, a_1, \dots, a_{2g+2})$ with $a_i \in \mathbf{Z}_p$ (resp. $a_i \in \mathbf{R}$) such that the curve (1) has genus g and has *no* $\mathbf{Q}_p$-rational point (resp. no real point). Finally we will use (3) with $S = \emptyset$.

The main point of Lemma 1 is to isolate (2) as the non-trivial condition that must be checked in order to obtain density results with infinitely many local conditions. The following result can be used to show that (2) is satisfied in many interesting cases.

Lemma 2. *Suppose f and g are relatively prime polynomials in $\mathbf{Z}[x_1, x_2, \dots, x_d]$. Let $S_M(f, g)$ be the set of $a \in \mathbf{Z}^d$ for which there exists a finite prime $p > M$ dividing both $f(a)$ and $g(a)$. Then $\lim_{M\to\infty} \overline{\rho}(S_M(f, g)) = 0$.*

Proof. See Section 3. □

Remark. Once one has Lemma 2, it is easy to apply Lemma 1 to obtain a formula for the density of $a \in \mathbf{Z}^d$ such that $f(a)$ and $g(a)$ are relatively prime, in terms of the number of solutions to $f(a) \equiv g(a) \equiv 0$ in $\mathbf{F}_p^d$ for each p. The same can of course be done for $\{a \in \mathbf{Z}^d : \gcd(f_1(a), \dots, f_n(a)) = 1\}$, provided that the polynomials $f_i \in \mathbf{Z}[x_1, \dots, x_d]$ define a subvariety of codimension at least 2 in $\mathbf{A}^d_{\mathbf{C}}$. This generalizes a result of Hafner, Sarnak, and McCurley [HSM].

[1] Since U_∞^1 is the union of the open set $(U_\infty^1)^0$ (its interior) and a subset of a measure zero set, U_∞^1 is automatically measurable.

For example, regarding the question we asked at the beginning, we obtain the following.

Lemma 3. *Fix $g \geq 1$. Let R_M be the set of $a = (a_0, a_1, \dots, a_{2g+2}) \in \mathbf{Z}^{2g+3}$ for which (1) is a curve X of genus g that fails to admit a $\mathbf{Q}_p$-rational point at some finite prime p greater than M. Then $\lim_{M \to \infty} \overline{\rho}(R_M) = 0$.*

Proof. An easy lemma [PSt, Lemma 15] shows that for p large compared to g, a necessary condition for the curve given by (1) to have no $\mathbf{Q}_p$–rational point is that the reduction of f mod p be a (non-square) constant times the square of some polynomial. If $g \geq 1$, then the Zariski closure[2] V of the image of the squaring map $\operatorname{Pol}_{g+1} \longrightarrow \operatorname{Pol}_{2g+2}$ (where Pol_n denotes the affine space of polynomials of degree $\leq n$) is of codimension at least 2 in $\operatorname{Pol}_{2g+2} = \mathbf{A}^{2g+3}$, so we can find two relatively prime polynomials $f, g \in \mathbf{Z}[a_0, \dots, a_{2g+2}]$ that vanish on V. For all but finitely many primes p, it is true that if $a \in \mathbf{Z}^{2g+3}$ and $f(x) \bmod p$ is a square in $\overline{\mathbf{F}}_p[x]$ then p divides $f(a)$ and $g(a)$. By Lemma 2, the claim follows. □

Lemma 3 supplies us with the condition (2) needed for the application of Lemma 1. We obtain the following answer to our question. Let ρ_g denote the density we asked for, and let $s_{g,v}$ be the s_v in Lemma 1 for the U_v (or U_∞) chosen in the paragraph after Lemma 1, so that $s_{g,v}$ is the 'probability' that the curve (1) with coefficients in $\mathbf{Z}_p$ (or $[-1, 1]$ for ∞) has *no* $\mathbf{Q}_p$-rational point (resp. no real point). Then

$$\rho_g = \prod_{v \in M_\mathbf{Q}} (1 - s_{g,v}),$$

and the product converges. Furthermore it is easy to show that $0 < s_{g,v} < 1$ for all $g \geq 1$ and for all v, so $0 < \rho_g < 1$.

Using Lemma 1, we could prove also that for any finite set S of places of $\mathbf{Q}$, and for any $g \geq 1$, there exists a genus g curve X over $\mathbf{Q}$ of the form (1) such that $\{v \in M_\mathbf{Q} : X(\mathbf{Q}_v) = \emptyset\} = S$ (and in fact, we would prove that such curves have positive density). A straightforward generalization of the method could be used to show that if K is any number field, S is any finite set of non-complex places of K, and $g \geq 1$, then there exists a genus g curve X over K of the form (1) such that $\{v \in M_K : X(K_v) = \emptyset\} = S$.

These last results fail for $g = 0$: it is well known that in addition $\#S$ must be even in order for there to exist X as above. The reason our method (luckily!) does not prove a false result for $g = 0$ is that (2) breaks down. More precisely, the proof of Lemma 3 fails for $g = 0$, since the image of the squaring map $\operatorname{Pol}_1 \to \operatorname{Pol}_2$ no longer has codimension at least 2.

3. Notes added in revision

We recently learned that T. Ekedahl developed in [Ek] very similar methods for computing densities when infinitely many local conditions are imposed. For instance, our Lemma 2 is a corollary of his Theorem 1.2, applied to the subscheme of $\mathbf{A}^d_\mathbf{Z}$ defined by the equations $f = g = 0$. Ekedahl gives applications of the method that are different from ours.

References

[Ek] Ekedahl, T., An infinite version of the Chinese remainder theorem, *Comment. Math. Univ. St. Paul.* **40** (1991), no. 1, 53–59.

[2] In fact, it is easy to show that the image of the squaring map is already Zariski closed, but we do not need this.

[HSM] Hafner, J., Sarnak, P., and McCurley, K., Relatively prime values of polynomials, *A tribute to Emil Grosswald: number theory and related analysis*, 437–443, *Contemp. Math.* **143**, Amer. Math. Soc., Providence, RI, 1993.

[PSt] Poonen, B. and Stoll, M., The Cassels–Tate pairing on polarized abelian varieties, preprint, 1998.

Department of Mathematics, University of California, Berkeley, CA 94720-3840, USA
E-mail address: poonen@math.berkeley.edu

Mathematisches Institut, Universität Düsseldorf, Universitätsstr. 1, D–40225 Düsseldorf, Germany.
E-mail address: stoll@math.uni-duesseldorf.de