ELECTRONIC RESEARCH ANNOUNCEMENTS
OF THE AMERICAN MATHEMATICAL SOCIETY
Volume 1, Issue 3, 1995

ON A QUANTITATIVE VERSION OF THE OPPENHEIM CONJECTURE.

ALEX ESKIN, GREGORY MARGULIS, AND SHAHAR MOZES

Abstract. The Oppenheim conjecture, proved by Margulis in 1986, states that the set of values at integral points of an indefinite quadratic form in three or more variables is dense, provided the form is not proportional to a rational form. In this paper we study the distribution of values of such a form. We show that if the signature of the form is not $(2,1)$ or $(2,2)$ then the values are uniformly distributed on the real line, provided the form is not proportional to a rational form. In the cases where the signature is $(2,1)$ or $(2,2)$ we show that no such universal formula exists, and give asymptotic upper bounds which are in general best possible.

Let Q be an indefinite nondegenerate quadratic form in n variables. Let $\mathcal{L}_Q = Q(\mathbb{Z}^n)$ denote the set of values of Q at integral points. The Oppenheim conjecture, proved by Margulis (cf. [Mar]) states that if $n \geq 3$, and Q is not proportional to a form with rational coefficients, then $\mathcal{L}_Q$ is dense. The Oppenheim conjecture enjoyed attention and many studies since it was conjectured in 1929 mostly using analytic number theory methods. In this paper[1] we study some finer questions related to the distribution the values of Q at integral points.

§1. Let ν be a continuous positive function on the sphere $\{v \in \mathbb{R}^n \mid \|v\| = 1\}$, and let $\Omega = \{v \in \mathbb{R}^n \mid \|v\| < \nu(v/\|v\|)\}$. We denote by $T\Omega$ the dilate of Ω by T. Define the following set:

$$V^Q_{(a,b)}(\mathbb{R}) = \{x \in \mathbb{R}^n \mid a < Q(x) < b\}$$

We shall use $V_{(a,b)} = V^Q_{(a,b)}$ when there is no confusion about the form Q. Also let $V_{(a,b)}(\mathbb{Z}) = V^Q_{(a,b)}(\mathbb{Z}) = \{x \in \mathbb{Z}^n \mid a < Q(x) < b\}$. The set $T\Omega \cap \mathbb{Z}^n$ consists of $O(T^n)$ points, $Q(T\Omega \cap \mathbb{Z}^n)$ is contained in an interval of the form $[-\mu T^2, \mu T^2]$, where $\mu > 0$ is a constant depending on Q and Ω. Thus one might expect that for any interval $[a, b]$, as $T \to \infty$,

$$|V_{(a,b)}(\mathbb{Z}) \cap T\Omega| \sim c_{Q,\Omega}(b-a)T^{n-2} \tag{1.1}$$

where $c_{Q,\Omega}$ is a constant depending on Q and Ω. This may be interpreted as "uniform distribution" of the sets $Q(\mathbb{Z}^n \cap T\Omega)$ in the real line. Our main result is

Received by the editors December 6, 1995.
1991 *Mathematics Subject Classification.* Primary 11J25, 22E40.
Research of the first author partially supported by an NSF postdoctoral fellowship and by BSF grant 94-00060/1.
Research of the second author partially supported by NSF grants DMS-9204270 and DMS-9424613.
Research of the third author partially supported by the Israel Science foundation and by BSF grant 94-00060/1.

[1]The full version is available electronically at `http://www.math.uchicago.edu/~eskin`

that (1.1) holds if Q is not proportional to a rational form, and has signature (p,q) with $p \geq 3$, $q \geq 1$. We also determine the constant $c_{Q,\Omega}$.

If Q is an indefinite quadratic form in n variables, Ω is as above and (a,b) is an interval, we show that there exists a constant $\lambda = \lambda_{Q,\Omega}$ so that as $T \to \infty$,

$$\mathrm{Vol}(V_{(a,b)}(\mathbb{R}) \cap T\Omega) \sim \lambda_{Q,\Omega}(b-a)T^{n-2} \tag{1.2}$$

Our main result is the following:

Theorem 1. *Let Q be an indefinite quadratic form of signature (p,q), with $p \geq 3$ and $q \geq 1$. Suppose Q is not proportional to a rational form. Then for any interval (a,b), as $T \to \infty$,*

$$|V_{(a,b)}(\mathbb{Z}) \cap T\Omega| \sim \lambda_{Q,\Omega}(b-a)T^{n-2}$$

where $n = p+q$, and $\lambda_{Q,\Omega}$ is as in (1.2).

Only the upper bound in this formula is new: the asymptotically exact lower bound was proved in [DM]. Also a lower bound with a smaller constant was obtained independently by M. Ratner, and by S. G. Dani jointly with S. Mozes (both unpublished).

If the signature of Q is $(2,1)$ or $(2,2)$ then no universal formula like (1.1) holds. In fact, we have the following theorem:

Theorem 2. *Let Ω_0 be the unit ball, and let $q = 1$ or 2. Then for every $\epsilon > 0$ and every interval (a,b) there exists a quadratic form Q of signature $(2,q)$ not proportional to a rational form, and a constant $c > 0$ such that for an infinite sequence $T_j \to \infty$,*

$$|V_{(a,b)}(\mathbb{Z}) \cap T\Omega_0| > cT_j^q(\log T_j)^{1-\epsilon}.$$

The case $q = 1$, $b \leq 0$ of Theorem 2 was noticed by P. Sarnak and worked out in detail in [Bre]. The quadratic forms constructed are of the form $x_1^2 + x_2^2 - \alpha x_3^2$, or $x_1^2 + x_2^2 - \alpha(x_3^2 + x_4^2)$, where α is extremely well approximated by squares of rational numbers.

However in the $(2,1)$ and $(2,2)$ cases, we can still establish an upper bound of the form $cT^q \log T$. This upper bound is effective, and is uniform over compact sets in the set of quadratic forms. We also give an effective uniform upper bound for the case $p \geq 3$.

Theorem 3. *Let $\mathcal{O}(p,q)$ denote the space of quadratic forms of signature (p,q) and discriminant ± 1, let $n = p+q$, (a,b) be an interval, and let $\mathcal{D}$ be a compact subset of $\mathcal{O}(p,q)$. Let ν be a continuous positive function on the unit sphere and let $\Omega = \{v \in \mathbb{R}^n \mid \|v\| < \nu(v/\|v\|)\}$. Then, if $p \geq 3$ there exists a constant c depending only on $\mathcal{D}$, (a,b) and Ω such that for any $Q \in \mathcal{D}$ and all $T > 1$,*

$$|V_{(a,b)}(\mathbb{Z}) \cap T\Omega| < cT^{n-2}$$

If $p = 2$ and $q = 1$ or $q = 2$, then there exists a constant $c > 0$ depending only on $\mathcal{D}$, (a,b) and Ω such that for any $Q \in \mathcal{D}$ and all $T > 2$,

$$|V_{(a,b)} \cap T\Omega \cap \mathbb{Z}^n| < cT^{n-2}\log T$$

Also, for the $(2,1)$ and $(2,2)$ cases, we have the following "almost everywhere" result:

Theorem 4. *For almost all quadratic forms Q of signature $(p,q) = (2,1)$ or $(2,2)$*

$$|V_{(a,b)}(\mathbb{Z}) \cap T\Omega| \sim \lambda_{Q,\Omega}(b-a)T^{n-2}$$

where $n = p+q$, and $\lambda_{Q,\Omega}$ is as in (1.2).

Theorem 4 may be proved using a recent general result of Nevo and Stein [NS]; we present a self-contained argument which suffices for the application in the full paper. In [Sar], P. Sarnak proved that an analogous asymptotic formula holds for almost all forms within a specific two-parameter family; this family arises in problems related to Quantum Chaos.

Finally, following [DM] we give a "uniform" version of Theorem 1:

Theorem 5. *Let $\mathcal{D}$ be a compact subset of $\mathcal{O}(p,q)$, with $p \geq 3$. Let $n = p+q$, and let Ω be as in Theorem 3. Then for every interval $[a,b]$ and every $\theta > 0$, there exists a finite subset $\mathcal{P}$ of $\mathcal{D}$ such that each $Q \in \mathcal{P}$ is a scalar multiple of a rational form and for any compact subset $\mathcal{F}$ of $\mathcal{D} - \mathcal{P}$ there exists T_0 such that for all Q in $\mathcal{F}$ and $T \geq T_0$,*

$$(1-\theta)\lambda_{Q,\Omega}(b-a)T^{n-2} \leq |V_{(a,b)}(\mathbb{Z}) \cap T\Omega| \leq (1+\theta)\lambda_{Q,\Omega}(b-a)T^{n-2}$$

where $\lambda_{Q,\Omega}$ is as in (1.2).

As in Theorem 1 only the upper bound is new; the asymptotically exact lower bound, which holds even for $SO(2,1)$ and $SO(2,2)$, was proved in [DM].

Remark 1. If we consider $|V_{(a,b)}(\mathbb{R}) \cap T\Omega \cap \mathcal{P}(\mathbb{Z}^n)|$ instead of $|V_{(a,b)}(\mathbb{Z}) \cap T\Omega|$ (where $\mathcal{P}(\mathbb{Z}^n)$ denotes the set of primitive lattice points, then Theorem 1 and Theorem 5 hold provided one replaces $\lambda_{Q,\Omega}$ by $\lambda'_{Q,\Omega} = \lambda_{Q,\Omega}/\zeta(n)$, where ζ is the Riemann zeta function.

Remark 2. Theorem 1 and Theorem 5, as well as lower bounds in [DM] and even the proof of the Oppenheim conjecture in [Mar], are not effective. It seems to be a very difficult problem to give effective versions of these results.

Passage to the space of lattices. We now relate the counting problem of Theorem 1 to a certain integral expression involving the orthogonal group of the quadratic form and the space of lattices $SL(n,\mathbb{R})/SL(n,\mathbb{Z})$. Roughly this is done as follows. Let f be a bounded function on $\mathbb{R}^n - \{0\}$ vanishing outside a compact subset. For $g \in SL(n,\mathbb{R})$ let

$$\tilde{f}(g) = \sum_{v \in \mathbb{Z}^n} f(gv) \tag{1.3}$$

The proof is based on the identity of the form

$$\int_K \tilde{f}(a_t k)\, dk = \sum_{v \in \mathbb{Z}^n} \int_K f(a_t k v)\, dk \tag{1.4}$$

obtained by integrating (1.3). In (1.4) $\{a_t\}$ is a certain diagonal subgroup of the orthogonal group of Q, and K is a maximal compact subgroup of the orthogonal group of Q. Then for an appropriate function f, the right hand side is then related to the number of lattice points $v \in [e^t/2, e^t]\partial\Omega$ with $a < Q(v) < b$. We then establish the asymptotics of the left-hand side using the ergodic theory of unipotent flows and some other techniques.

Lattices. Let Δ be a lattice in $\mathbb{R}^n$. We say that a subspace L of $\mathbb{R}^n$ is Δ-*rational* if $L \cap \Delta$ is a lattice in L. For any Δ-rational subspace L, we denote by $d_\Delta(L)$ or simply by $d(L)$ the volume of $L/(L\cap\Delta)$. Let us note that $d(L)$ is equal to the norm of $e_1 \wedge \cdots \wedge e_\ell$ in the exterior power $\bigwedge^\ell(\mathbb{R}^n)$ where $\ell = \dim L$ and $(e_1, \cdots, e_\ell)$ is a basis over $\mathbb{Z}$ of $L \cap \Delta$. If $L = \{0\}$ we write $d(L) = 1$. A lattice is Δ *unimodular* if $d_\Delta(\mathbb{R}^n) = 1$. The space of unimodular lattices is isomorphic to $SL(n,\mathbb{R})/SL(n,\mathbb{Z})$.

Let us introduce the following notation:

$$\alpha_i(\Delta) = \sup\left\{\frac{1}{d(L)}\,\middle|\, L \text{ is a } \Delta\text{-rational subspace of dimension } i\right\}, \quad 0 \le i \le n,$$
$$\alpha(\Delta) = \max_{0\le i\le n} \alpha_i(\Delta).$$

The following lemma is known as the “Lipshitz Principle”:

Lemma ([Sch, Lemma 2]). *Let f be a bounded function on $\mathbb{R}^n$ vanishing outside a compact subset. Then there exists a positive constant $c = c(f)$ such that*

$$\tilde{f}(\Delta) < c\alpha(\Delta) \tag{1.5}$$

for any lattice Δ in $\mathbb{R}^n$. Here $\tilde{f}$ is the function on the space of lattices defined in (1.3).

Quadratic Forms. Let $n \ge 3$, and let $p \ge 2$. We denote $n-p$ by q, and assume $q > 0$. Let $\{e_1, e_2, \ldots e_n\}$ be the standard basis of $\mathbb{R}^n$. Let Q_0 be the quadratic form defined by

$$Q_0\left(\sum_{i=1}^n v_i e_i\right) = 2v_1 v_n + \sum_{i=2}^p v_i^2 - \sum_{i=p+1}^{n-1} v_i^2 \quad \text{for all } v_1, \ldots, v_n \in \mathbb{R}.$$

It is straightforward to verify that Q_0 has signature (p,q). Let $G = SL(n,\mathbb{R})$, the group of $n\times n$ matrices of determinant 1. For each quadratic form Q and $g \in G$, let Q^g denote the quadratic form defined by $Q^g(v) = Q(gv)$ for all $v \in \mathbb{R}^n$. By the well known classification of quadratic forms over $\mathbb{R}$, for each $Q \in \mathcal{O}(p,q)$ there exists $g \in G$ such that $Q = Q_0^g$. For any quadratic form Q let $SO(Q)$ denote the special orthogonal group corresponding to Q; namely $\{g \in G \mid Q^g = Q\}$. Let $H = SO(Q_0)$. Then the map $H\backslash G \to \mathcal{O}(p,q)$ given by $Hg \to Q_0^g$ is a homeomorphism.

For $t \in \mathbb{R}$, let a_t be the linear map so that $a_t e_1 = e^{-t}e_1$, $a_t e_n = e^t e_n$, and $a_t e_i = e_i$, $2 \le i \le n-1$. Then the one-parameter group $\{a_t\}$ is contained in H. Let $\hat{K}$ be the subgroup of G consisting of orthogonal matrices, and let $K = H \cap \hat{K}$. It is easy to check that K is a maximal compact subgroup of H, and consists of all $h \in H$ leaving invariant the subspace spanned by $\{e_1 + e_n, e_2, \ldots, e_p\}$. We denote by m the normalized Haar measure on K.

The main theorems. To prove Theorem 1 one may use the following theorem:

Theorem 6. *Suppose $p \ge 3$, $q \ge 1$. Let ϕ be a continuous function on $G/\Gamma \approx$ the space of lattices in $\mathbb{R}^n$ with determinant 1. Assume that for some s, $0 < s < 2$ and some $C > 0$,*

$$|\phi(\Delta)| < C\alpha(\Delta)^s, \qquad \textit{for all } \Delta \in G/\Gamma$$

Let $x_0 \in G/\Gamma$ be a unimodular lattice such that Hx_0 is not closed. Let ν be any continuous function on K. Then

$$\lim_{t\to+\infty} \int_K \phi(a_t k x_0)\nu(k)\, dm(k) = \int_K \nu\, dm \int_{G/\Gamma} \phi(y)\, d\mu(y).$$

To prove Theorem 5 we use the following generalization:

Theorem 7. *Suppose $p \geq 3$, $q \geq 1$. Let ϕ, ν be as in Theorem 6, and let $\mathcal{C}$ be any compact set in G/Γ. Then for any $\epsilon > 0$ there exist finitely many points $x_1, \dots, x_\ell \in G/\Gamma$ such that*

(i) *The orbits $Hx_1, \dots, Hx_\ell$ are closed and have finite H-invariant measure.*
(ii) *For any compact subset F of $\mathcal{C} - \bigcup_{1\leq i\leq \ell} Hx_i$, there exists $t_0 > 0$, so that for all $x \in F$ and $t > t_0$,*

$$\left| \int_K \phi(a_t k x)\nu(k)\, dm(k) - \int_{G/\Gamma} \phi\, d\mu \int_K \nu\, dm \right| \leq \epsilon$$

If the function ϕ is bounded, then Theorem 6 and Theorem 7 follow easily from [DM, Theorem 3]). This theorem is a refined version of Ratner's uniform distribution theorem [Rat4]; the proof uses Ratner's measure classification theorem (see [Rat1, Rat2, Rat3]), Dani's theorem on the behavior of unipotent orbits at infinity [Dan1, Dan2], and "linearization" techniques.

Both [DM, Theorem 3] and Ratner's uniform distribution theorem hold for bounded continuous functions, but not for arbitrary continuous functions from $L^1(G/\Gamma)$. However, for a non-negative bounded continuous function f on $\mathbb{R}^n$, the function $\tilde{f}$ defined in (1.3) is non-negative, continuous, and L^1 but unbounded (it is in $L^s(G/\Gamma)$ for $1 \leq s < n$, where $G = SL(n, \mathbb{R})$, and $\Gamma = SL(n, \mathbb{Z})$). As it was done in [DM] it is possible to obtain asymptotically exact lower bounds by considering bounded continuous functions $\phi \leq \tilde{f}$. However, to carry out the integrals in (1.4) and prove the upper bounds in the theorems stated above we need to examine carefully the situation at the "cusp" of G/Γ, i.e outside of compact sets.

By (1.5) the function $\tilde{f}(g)$ on the space of unimodular lattices G/Γ is majorized by the function $\alpha(g)$. The function α is more convenient since it is invariant under the left action of the maximal compact subgroup $\hat{K}$ of G, and its growth rate at infinity is known explicitly. Theorems 1 and 5 are proved by combining [DM, Theorem 3] with the following integrability estimate:

Theorem 8. *If $p \geq 3$, $q \geq 1$ and $0 < s < 2$, or if $p = 2$, $q \geq 1$ and $0 < s < 1$, then for any lattice Δ in $\mathbb{R}^n$*

$$\sup_{t>0} \int_K \alpha(a_t k \Delta)^s\, dm(k) < \infty.$$

The upper bound is uniform as Δ varies over compact sets in the space of lattices.

This result can be interpreted as follows. For a lattice Δ in G/Γ and for $h \in H$, let $f(h) = \alpha(h\Delta)$. Since α is left-$\hat{K}$ invariant, f is a function on the symmetric space $X = K\backslash H$. Theorem 8 is the statement that if if $p \geq 3$, then the averages of f^s, $0 < s < 2$ over the sets Ka_tK in X remain bounded as $t \to \infty$, and the bound is uniform as one varies the base point Δ over compact sets. We remark that in the case $q = 1$, the rank of X is 1, and the sets Ka_tK are metric spheres of radius t, centered at the origin.

If $(p, q) = (2, 1)$ or $(2, 2)$, Theorem 8 does not hold even for $s = 1$. The following result is, in general, best possible:

Theorem 9. *If $p = 2$ and $q = 2$, or if $p = 2$ and $q = 1$, then for any lattice Δ in $\mathbb{R}^n$,*

$$\sup_{t>1} \frac{1}{t} \int_K \alpha(a_t k\Delta)\, dm(k) < \infty,$$

The upper bound is uniform as Δ varies over compact sets in the space of lattices.

§2. We now outline the proof of Theorems 8 and 9. From its definition, the function $\alpha(g)$ is the maximum over $1 \leq i \leq n$ of left-$\hat{K}$ invariant functions $\alpha_i(g)$. The main idea of the proof is to show that the α_i satisfy a system of integral inequalities which imply the desired bound.

If $p \geq 3$ and $0 < s < 2$, or if $(p, q) = (2, 1)$ or $(2, 2)$ and $0 < s < 1$, we show that for any $c > 0$ there exist $t > 0$, and $\omega > 1$ so that the the functions α_i^s satisfy the following system of integral inequalities in the space of lattices:

$$A_t \alpha_i^s \leq c_i \alpha_i^s + \omega^2 \max_{0 \leq j \leq n-i, i} \sqrt{\alpha_{i+j}^s \alpha_{i-j}^s} \tag{2.1}$$

where A_t is the averaging operator $(A_t f)(\Delta) = \int_K f(a_t k\Delta)$, and $c_i \leq c$. If $(p, q) = (2, 1)$ or $(2, 2)$ and $s = 1$, then (2.1) also holds (for suitably modified functions α_i), but some of the constants c_i cannot be made smaller than 1.

Let $f_i(h) = \alpha_i(h\Delta)$, so that each f_i is a function on the symmetric space X. When one restricts to an orbit of H, (2.1) becomes:

$$A_t f_i^s \leq c_i f_i^s + \omega^2 \max_{0 \leq j \leq n-i, i} \sqrt{f_{i+j}^s f_{i-j}^s} \tag{2.2}$$

If $\operatorname{rank} X = 1$, then $(A_t f)(h)$ can be interpreted as the average of f over the sphere of radius t in X, centered at h. We show that if the f_i satisfy (2.2) then for any $\epsilon > 0$, the function $f = f_{\epsilon,s} = \sum_{0 \leq i \leq n} \epsilon^{i(n-i)} f_i^s$ satisfies the scalar inequality:

$$A_t f \leq cf + b \tag{2.3}$$

where t, c and b are constants. We show that if c is sufficiently small, then (2.3) for a fixed t together with the uniform continuity of $\log f$ imply that $(A_r f)(1)$ is bounded as a function of r, which is the conclusion of Theorem 8. If $c = 1$, which will occur in the $SO(2, 1)$ and $SO(2, 2)$ cases, then (2.3) implies that $(A_r f)(1)$ is growing at most linearly with the radius, which is the conclusion of Theorem 9.

Throughout the proof we consider the functions $\alpha(g)^s$ for $0 < s < 2$ even though for the application to quadratic forms we only need $s = 1 + \delta$. This yields a better integrability result, and is also necessary for the proofs of Theorem 6 and Theorem 7.

Acknowledgments: The authors would like to thank Peter Sarnak for useful conversations.

References

[Bre] T. Brennan. . Princeton University undergraduate thesis, 1994.

[Dan1] S.G. Dani. On orbits of unipotent flows on homogeneous spaces. *Ergod. Theor. Dynam. Syst.* **4**(1984), 25–34.

[Dan2] S.G. Dani. On orbits of unipotent flows on homogenous spaces II. *Ergod. Theor. Dynam. Syst* **6**(1986), 167–182.

[DM] S.G. Dani and G.A. Margulis. Limit distributions of orbits of unipotent flows and values of quadratic forms. *Advances in Soviet Math.* **16**(1993), 91–137.

[Mar] G. A. Margulis. Discrete Subgroups and Ergodic Theory. In *Number theory, trace formulas and discrete subgroups (a symposium in honor of A. Selberg)*, pages 377–398. Academic Press, Boston, MA, 1989.

[NS] A. Nevo and E. Stein. A generalization of Wiener's pointwise ergodic theorem. Preprint.

[Rat1] M. Ratner. Strict measure rigidity for nilpotent subgroups of solvable groups. *Invent. Math.* **101**(1990), 449–482.

[Rat2] M. Ratner. On measure rigidity of unipotent subgroups of semisimple groups. *Acta. Math.* **165**(1990), 229–309.

[Rat3] M. Ratner. On Raghunathan's measure conjecture. *Annals of Math.* **134**(1991), 545–607.

[Rat4] M. Ratner. Raghunathan's topological conjecture and distributions of unipotent flows. *Duke Math. J.* **63**(1991), 235–290.

[Sch] W. Schmidt. Asymptotic formulae for point lattices of bounded determinant and subspaces of bounded height. *Duke Math. J.* **35**(1968), 327–339.

[Sar] P. Sarnak. Values at integers of binary quadratic forms. In preparation.

Department of Mathematics, University of Chicago, Chicago IL 60637, USA
E-mail address: eskin@math.uchicago.edu

Department of Mathematics, Yale University, New Haven CT, USA
E-mail address: margulis@math.yale.edu

Institute of Mathematics, Hebrew University, Jerusalem 91904, ISRAEL
E-mail address: mozes@math.huji.ac.il