Forum of Mathematics, Sigma (2014), Vol. 2, e13, 8 pages
doi:10.1017/fms.2014.10

COUNTING S_5-FIELDS WITH A POWER SAVING ERROR TERM

ARUL SHANKAR and JACOB TSIMERMAN
Harvard University, Department of Mathematics, One Oxford Street, Cambridge, MA 02138, USA;
email: arul.shnkr@gmail.com

Received 19 November 2013; accepted 26 March 2014

Abstract

We show how the Selberg Λ^2-sieve can be used to obtain power saving error terms in a wide class of counting problems which are tackled using the geometry of numbers. Specifically, we give such an error term for the counting function of S_5-quintic fields.

2010 Mathematics Subject Classification: primary 13N15; secondary 16S36, 16W55.

1. Introduction

Over the past decade there has emerged a large body of work concerned with counting arithmetic objects by parameterizing them as $G_{\mathbb{Z}}$ orbits on $V_{\mathbb{Z}}$, where G is some reductive algebraic group, and V is a representation of G (see [3, 5–9, 11]). In certain applications, particularly relating to low lying zeros–see [12], it is important not only to obtain the asymptotic count, but also to obtain a power saving error term, that is a formula of the type

$$\#\{\text{Objects of interest with height less than } X\} = cX^a \log^b X + O(X^{a-\delta})$$

for some fixed constant $\delta > 0$.

In this note, we show how the Selberg Λ^2-sieve can be used very generally to obtain such power savings. In particular, we demonstrate our claim by obtaining the first known power saving for quintic fields with Galois group S_5 and bounded discriminant:

THEOREM 1. *Define* $N_5^{(i)}(X)$ *to be the number of quintic fields with Galois group* S_5 *having discriminant bounded in absolute value by* X *with* i *complex places. Then*

$$N_5^{(i)}(X) = d_i \prod_p (1 + p^{-2} - p^{-4} - p^{-5})X + O_\epsilon(X^{\frac{199}{200}+\epsilon})$$

where d_0, d_1, d_2 *are* $1/240$, $1/24$, *and* $1/16$, *respectively.*

The analogous version of Theorem 1 in the case for cubic and quartic fields with Galois groups S_3 and S_4, respectively, was proven in [2]. However, in those cases, the arguments used to obtain power saving error estimates were explicit and do not easily generalize. An advantage to using the Selberg Λ^2-sieve is that it is very general. It yields power saving error estimates when counting the arithmetic objects that arise in, for example, [7, 9, 11].

We begin with a general sketch of the argument.

1.1. Sketch of the argument. Typically, one finds a fundamental domain $F \subset V_{\mathbb{R}}$ for the action of $G_{\mathbb{R}}$, and one wants to count integral points inside F of bounded height. However, it is not all points that one wants to count; one partitions the set $V_{\mathbb{Z}}$ into two sets $V_{\mathbb{Z}}^{\text{deg}}$ and $V_{\mathbb{Z}}^{\text{ndeg}}$ where the former set corresponds to objects which are 'degenerate' in some way, and it is only the points in $V_{\mathbb{Z}}^{\text{ndeg}}$ that need to be counted. For example, in the quintic case the degenerate points correspond to quintic rings R such that $R \otimes_{\mathbb{Z}} \mathbb{Q}$ is not a quintic field with Galois group S_5. F is typically not compact and has 'cusps' which contain primarily degenerate points; the method which one uses to estimate the number of nondegenerate points in the cusp typically yields a power saving. Denoting the 'main ball' of F by F_0, and letting $F_0(X)$ be the set of points in F_0 having height at most X, it then follows that

$$|V_{\mathbb{Z}} \cap F_0(X)| = cX^a \log^b X + O(X^{a-\delta}).$$

It remains to estimate the number of degenerate points inside the main body $F_0 \subset F$, and it is in this last estimate that past results have frequently failed to obtain a power saving.

The typical argument runs as follows. The reduction modulo a prime p of $V_{\mathbb{Z}}^{\text{deg}}$ is shown to lie in a subset $B_p \subset V_{\mathbb{F}_p}$ of density μ_p, which approaches a constant c between 0 and 1 as $p \to \infty$. Set $\widetilde{B}_p$ to be the set of elements of $V_{\mathbb{Z}}$ reducing to B_p. For any finite fixed set S of primes, one has the estimate

$$|V_{\mathbb{Z}}^{\text{deg}} \cap F_0(X)| \leqslant \left| \bigcap_{p\in S} \widetilde{B}_p \cap F_0(X) \right| \sim \prod_{p\in S} \mu_p \cdot cX^a \log^b X.$$

This is true for every fixed S. Since $\prod_{p\in S}\mu_p$ can be made arbitrarily small by picking S to be a large set, one obtains

$$|V_{\mathbb{Z}}^{\deg} \cap F_0(X)| = o(X^a \log^b X).$$

However it is possible to do much better by estimating $|\bigcap_{p\in S} \widetilde{B}_p|$ with the Selberg sieve [10, Theorem 6.4]. To apply this sieve, we need the following uniform statement. Let $L \subset V_{\mathbb{Z}}$ be defined by congruence conditions modulo m. Then

$$|L \cap F_0(X)| = \mu(L)cX^a \log^b X + O(X^{a-\delta}m^A),$$

where $\mu(L)$ denotes the density of L in $V_{\mathbb{Z}}$, and A is a fixed constant independent of L. The application of the Selberg sieve immediately yields a power saving error term:

$$|V_{\mathbb{Z}}^{\deg} \cap F_0(X)| = O_\epsilon(X^{a-\frac{\delta}{2A+3}+\epsilon}).$$

We remark that for arithmetic applications one usually needs a further sieve (for example, a sieve from quintic rings to maximal quintic rings). This can be done with a power saving error term following [2].

1.2. Outline of the paper. In Section 2, we collect the arguments used by Bhargava in [5] to parameterize and count the number of quintic rings of a bounded discriminant. In Section 3 we use the Selberg sieve to obtain a power saving estimate for the number of non-S_5-orders having bounded discriminant. We try to adhere to the notation of [10, Theorem 6.4] for the convenience to the reader. In Section 4 we prove our main theorem by sieving down from S_5-orders to S_5-fields.

2. S_5-quintic orders

In this section, we recall results from [5] that allow us to obtain asymptotics for the number of S_5-quintic orders having bounded discriminant. All the results and the notation in this section directly follow [5].

2.1. Parameterizing quintic rings. Let $V_{\mathbb{Z}}$ denote the space of quadruples of 5×5 skew-symmetric matrices with integer coefficients. The group $G_{\mathbb{Z}} := \mathrm{GL}_4(\mathbb{Z}) \times \mathrm{SL}_5(\mathbb{Z})$ acts on $V_{\mathbb{Z}}$ via $(g_4, g_5) \cdot (A, B, C, D)^t = g_4(g_5 A g_5^t, g_5 B g_5^t, g_5 C g_5^t, g_5 D g_5^t)^t$. The ring of invariants for this action is generated by one element, denoted as the discriminant. In [4], Bhargava shows that quintic rings are parameterized by $G_{\mathbb{Z}}$-orbits on $V_{\mathbb{Z}}$:

https://doi.org/10.1017/fms.2014.10 Published online by Cambridge University Press

THEOREM 2 (Bhargava [4]). *There is a canonical bijection between the set of $G_{\mathbb{Z}}$-orbits on elements $(A, B, C, D) \in V_{\mathbb{Z}}$ and the set of isomorphism classes of pairs (R, R'), where R is a quintic ring and R' is a sextic resolvent of R. Under this bijection, we have* $\mathrm{Disc}(A, B, C, D) = \mathrm{Disc}(R) = (1/16)\mathrm{Disc}(R')^{1/3}$.

2.2. Counting quintic rings. Following [5], we say that an element $v \in V_{\mathbb{Z}}$ is *irreducible* if it corresponds to a pair of rings (R, R') such that R is an integral domain. For a $G_{\mathbb{Z}}$-invariant subset S of $V_{\mathbb{Z}}$, let $N(S, X)$ denote the number of irreducible $G_{\mathbb{Z}}$-orbits on S having discriminant bounded by X.

The quantity $N(V_{\mathbb{Z}}; X)$ is estimated in the following way: the action of $G_{\mathbb{R}}$ on $V_{\mathbb{R}}$ has three open orbits denoted as $V_{\mathbb{R}}^{(0)}$, $V_{\mathbb{R}}^{(1)}$, and $V_{\mathbb{R}}^{(2)}$. Let $\mathcal{F}$ be a fundamental domain for the action of $G_{\mathbb{Z}}$ on $G_{\mathbb{R}}$ and let H be an open bounded set in $V_{\mathbb{R}}^{(i)}$. Denote $V_{\mathbb{Z}} \cap V_{\mathbb{R}}^{(i)}$ by $V_{\mathbb{Z}}^{(i)}$, and let $S \subset V_{\mathbb{Z}}^{(i)}$ be a $G_{\mathbb{Z}}$-invariant subset. Then by [5, Equations (9) and (10)], we have

$$\begin{aligned} N(S, X) &= \frac{\displaystyle\int_{v\in H} \#\{x \in \mathcal{F}v \cap S^{\mathrm{irr}} : |\mathrm{Disc}(x)| < X\}|\mathrm{Disc}(v)|^{-1} dv}{\displaystyle n_i \int_{v\in H} |\mathrm{Disc}(v)|^{-1} dv} \\ &= C_i \int_{g\in\mathcal{F}} \#\{x \in gH \cap S^{\mathrm{irr}} : |\mathrm{Disc}(x)| < X\} dg, \end{aligned} \tag{1}$$

where dg is the Haar measure on $G_{\mathbb{R}}$ and S^{irr} denotes the set of irreducible elements in S. Note that n_i depends only on i and C_i is independent of S. In what follows, we pick $\mathcal{F}$ and dg as in [5, Section 2.1]. Once they are picked, we let (1) define $N(S, X)$ even for sets S that are not $G_{\mathbb{Z}}$-invariant. Define also the related quantity $N^*(S, X)$ via

$$N^*(S, X) := C_i \int_{g\in\mathcal{F}} \#\{x \in gH \cap S : |\mathrm{Disc}(x)| < X\} dg.$$

For $G_{\mathbb{Z}}$-invariant sets S, the quantity $N^*(S, X)$ is the number of (not necessarily irreducible) $G_{\mathbb{Z}}$-orbits on S having discriminant bounded by X.

Let a_{12} denote the 12-coordinate of A. In [5], the set of elements in gH is partitioned into two sets: the set where $|a_{12}| \geqslant 1$ or the 'main ball' and the set where $|a_{12}| < 1$ or the 'cusp'. Then [5, Lemma 11] states that we have

$$N(\{x \in V_{\mathbb{Z}}^{(i)} : a_{12} = 0\}, X) = O(X^{\frac{39}{40}}). \tag{2}$$

Proposition 12 combined with the last equation in Section 2.6 of [5] implies that

$$N^*(\{x \in V_{\mathbb{Z}}^{(i)} : a_{12} \neq 0\}, X) = c_i X + O(X^{\frac{39}{40}}), \tag{3}$$

where

$$c_i := \frac{\zeta(2)^2\zeta(3)^2\zeta(4)^2\zeta(5)}{2n_i}.$$

To sieve down to fields, we will need analogous equations where $V_{\mathbb{Z}}^{(i)}$ is replaced by a set defined by finitely many congruence conditions on $V_{\mathbb{Z}}$. Specifically, if L is a translate of $mV_{\mathbb{Z}}$, then from [5, Equation 28] we have

$$N^*(\{x \in L \cap V_{\mathbb{Z}}^{(i)} : a_{12} \neq 0\}, X) = c_i m^{-40} X + O(m^{-39} X^{\frac{39}{40}}). \tag{4}$$

2.3. Congruence conditions for $V_{\mathbb{Z}}^{\mathrm{NS5}}$. Let $V_{\mathbb{Z}}^{\mathrm{S5}}$ denote the set of elements in $V_{\mathbb{Z}}$ that correspond to quintic orders whose field of fractions is an S_5-number field, and let $V_{\mathbb{Z}}^{\mathrm{NS5}}$ denote the complement of $V_{\mathbb{Z}}^{\mathrm{S5}}$ in $V_{\mathbb{Z}}$. As explained in [5, Section 3.2], there exist disjoint subsets $T_p(1112)$ and $T_p(5)$ of $V_{\mathbb{Z}}$, that are defined by congruence conditions modulo p, such that for any two distinct primes p and q, the set $V_{\mathbb{Z}}^{\mathrm{NS5}}$ is disjoint from $T_p(1112) \cap T_q(5)$. Furthermore, the densities $g_p(1112)$ of $T_p(1112)$ and $g_p(5)$ of $T_p(5)$ approach $1/12$ and $1/5$, respectively, as $p \to \infty$. We set $S_p(1112)$ and $S_p(5)$ as the complements of $T_p(1112)$ and $T_p(5)$ respectively.

3. Applying the Selberg sieve

Define

$$N_{12}^*(S, X) = N^*(\{x \in S : a_{12} \neq 0\}, X).$$

In this section we give a power saving estimate for $N_{12}^*(V_{\mathbb{Z}}^{\mathrm{NS5},(i)}, X)$. By Section 2.3, we know that

$$N_{12}^*(V_{\mathbb{Z}}^{\mathrm{NS5},(i)}, X) \leqslant N_{12}^*(\cap_p S_p(5), X) + N_{12}^*(\cap_p S_p(1112), X). \tag{5}$$

Our goal is to bound each of the two terms on the RHS of (5) using the Selberg sieve. We turn to the details. We begin by fixing a number $z < X$. Set $P(z) = \prod_{p<z} p$. For each square-free number $d \mid P(z)$, set $g_d(5) = \prod_{p|d} g_p(5)$ and

$$a_d = N_{12}^*\Bigg(\bigcap_{p|d} T_p(5) \bigcap_{p|\frac{P(z)}{d}} S_p(5), X\Bigg).$$

We define a_d to be 0 for $d \nmid P(z)$. This is a sequence of nonnegative integers, and by (4) we have that for all $d \mid P(z)$,

$$\sum_{n \equiv 0 \bmod d} a_n = N_{12}^*(\cap_{p|d} T_p(5), X) = c_i g_d(5) X + r_d \tag{6}$$

https://doi.org/10.1017/fms.2014.10 Published online by Cambridge University Press

where $r_d = O(dg_d(5)X^{39/40})$. Fix $D > 1$ and define

$$h_d(5) = \prod_{p|d} \frac{g_p(5)}{1 - g_p(5)}, \quad H = \sum_{\substack{d<\sqrt{D} \\ d|P(z)}} h_d(5).$$

A direct application of [10, Theorem 6.4] yields

$$a_1 = \sum_{(n,P(z))=1} a_n \leqslant c_i X H^{-1} + O\left(\sum_{d<D,d|P(z)} \tau_3(d) r_d\right). \tag{7}$$

To use (7) we take $z = \sqrt{X}$. Note that since $g_p(5) \to \frac{1}{5}$, we have

$$d^{-\epsilon} \ll_\epsilon g_d(5), h_d(5) \ll_\epsilon d^\epsilon.$$

It follows that $H = D^{\frac{1}{2}+o(1)}$ while

$$\left|\sum_{d<D,d|P(z)} \tau_3(d) r_d\right| \ll_\epsilon X^{\frac{39}{40}} D^\epsilon \sum_{d<D} d \leqslant X^{\frac{39}{40}} D^{2+\epsilon}.$$

We deduce that $a_1 \ll_\epsilon XD^{-1/2+\epsilon} + X^{39/40}D^{2+\epsilon}$. Optimizing, we take $D = X^{1/100}$ to deduce that $a_1 \ll_\epsilon X^{199/200+\epsilon}$.

It follows that

$$N_{12}^*(\cap_p S_p(5), X) \leqslant N_{12}^*(\cap_{p<z} S_p(5), X) = a_1 \ll_\epsilon X^{\frac{199}{200}+\epsilon}.$$

The case of $N^*(\cap_p S_p(1112), X)$ can be treated similarly, and we thus conclude by (5) that

$$N_{12}^*(V_{\mathbb{Z}}^{\mathrm{NS5},(i)}, X) \ll_\epsilon X^{\frac{199}{200}+\epsilon}. \tag{8}$$

4. Sieving to fields

In this section we follow [2] to prove Theorem 1. For d square-free, define $W_d \subset V_{\mathbb{Z}}$ to be the set of elements corresponding to quintic orders that are not maximal at each prime dividing d, and $U_d \subset V_{\mathbb{Z}}$ to be the complement of W_d. Recall from [5] that W_d is defined by congruence conditions modulo d^2.

We need a slight generalization of the uniformity estimate [5, Proposition 19].

LEMMA 3. $N(W_d, X) = O_\epsilon(X/d^{2-\epsilon})$.

Proof. As in [5, Proposition 19], we count rings that are not maximal by counting their over-rings. As in that proof, we use the result of Brakenhoff [1]

https://doi.org/10.1017/fms.2014.10 Published online by Cambridge University Press

that the number of orders having index m in a maximal quintic ring R is $\prod_{p^k||m} O(p^{\min(2k-2,20k/11)})$. Moreover, from [4, Proof of Corollary 4], the number of sextic resolvents of a quintic ring of content n is $O(n^6)$. (Recall that the content of a ring is the largest integer n such that $R = \mathbb{Z} + nR'$ for some quintic ring R'.)

Since $\mathrm{Disc}(R) = n^8 \mathrm{Disc}(R')$, we have

$$N(W_d, X) \ll_\epsilon d^\epsilon X \sum_{n=1}^{\infty} \frac{n^6}{n^8} \prod_{p|d} \sum_{k=1}^{\infty} \frac{p^{\min(2k-2, \frac{20k}{11})}}{p^{2k}} \ll_\epsilon X/d^{2-\epsilon}$$

as desired. □

Now, a point in $V_\mathbb{Z}$ corresponds to a maximal order in an S_5-field precisely if it is in $\cap_p U_p \cap V_\mathbb{Z}^{S5}$. Denote the density of W_d by k_d, and recall from [5] that $k_d = O_\epsilon(d^{-2+\epsilon})$. A quintic field is maximal if and only if it is maximal at all primes p, and so we count S_5-quintic fields by estimating the quantity $N(\cap_p U_p \cap V_\mathbb{Z}^{(i)}, X)$ as follows:

$$\begin{aligned}
N(\cap_p U_p \cap V_\mathbb{Z}^{(i)}, X) &= \sum_{d \in \mathbb{N}} \mu(d) N(W_d \cap V_\mathbb{Z}^{(i)}, X) \\
&= \sum_{d<T} \Big(c_i \mu(d) k_d X + O(X^{\frac{39}{40}} d^\epsilon)\Big) + \sum_{d>T} O_\epsilon(X/d^{2-\epsilon}) \\
&= \sum_{d \in \mathbb{N}} c_i \mu(d) k_d X + O_\epsilon(X/T^{1-\epsilon} + X^{\frac{39}{40}} T^{1+\epsilon}) \\
&= c_i \prod_p (1-k_p) X + O_\epsilon(X/T^{1-\epsilon} + X^{\frac{39}{40}} T^{1+\epsilon}).
\end{aligned}$$

Since W_d is the union of $O_\epsilon(d^{78+\epsilon})$ translates of $d^2 V_\mathbb{Z}$, the second equality follows from (4) and Lemma 3. Optimizing, we pick $T = X^{1/80}$ and, taking this in conjunction with (2) and (8), we obtain Theorem 1.

Acknowledgements

We are very grateful to Anders Södergren and the referees for many helpful comments on an earlier version of this manuscript, and for suggesting an argument that improved the magnitude of the power saving in the error term.

References

[1] J. Brakenhoff, ‘Counting problem for number rings’, PhD thesis, Lieden University, 2009.
[2] K. Belabas, M. Bhargava and C. Pomerance, ‘Error terms for the Davenport–Heilbronn theorems’, *Duke Math. J.* **153** (2010), 173–210.

[3] M. Bhargava, 'The density of discriminants of quartic rings and fields', *Ann. of Math.* **162** 1031–1063.

[4] M. Bhargava, 'Higher composition laws IV. The parametrization of quintic rings', *Ann. of Math.* **2** (1) (2008), 5394.

[5] M. Bhargava, 'The density of discriminants of quintic rings and fields', *Ann. of Math. 2* **172** (3) (2010), 1559–1591.

[6] M. Bhargava, 'Most hyperelliptic curves over Q have no rational points', arXiv:1308.0395.

[7] M. Bhargava and B. Gross, 'The average size of the 2-Selmer group of Jacobians of hyperelliptic curves having a rational Weierstrass point', 2012, arXiv:1208.1007.

[8] M. Bhargava and A. Shankar, 'Binary quartic forms having bounded invariants, and the boundedness of the average rank of elliptic curves', Preprint.

[9] M. Bhargava and A. Shankar, 'The average number of elements in the 5-Selmer group of elliptic curves' (in preparation).

[10] H. Iwaniec and E. Kowalski, *Analytic Number Theory*, Amer. Math. Soc. Colloq. Publ., 53 (Amer. Math. Soc., Providence, RI, 2004).

[11] A. Shankar and X. Wang, 'The average size of the 2-Selmer group for monic even hyperelliptic curves', arXiv:1307.3531.

[12] A. Yang, 'Distribution problems associated to zeta functions and invariant theory', PhD thesis, Princeton University, 2009.

https://doi.org/10.1017/fms.2014.10 Published online by Cambridge University Press