Average distribution of prime ideals in families of number fields

Igor E. Shparlinski
Department of Computing, Macquarie University
Sydney, NSW 2109, Australia
igor@ics.mq.edu.au
José Felipe Voloch
Department of Mathematics, University of Texas
Austin TX 78712 USA
voloch@math.utexas.edu

May 22, 2007

Abstract

We view an algebraic curve over $\mathbb{Q}$ as providing a one-parameter family of number fields and obtain bounds for the average value of some standard prime ideal counting functions over these families which are better than averaging the standard estimates for these functions.

2000 Mathematics Subject Classification: 11R44

Keywords: Prime ideal theorem, Chebotarev density Theorem, Families of number fields.

1 Introduction

Let $f(x, y)$ be a general polynomial with integer coefficients and, for an integer $a > 0$ such that $f(a, y)$ is irreducible let $\mathbb{K}_a$ be the number field generated by a root of $f(a,y)=0$ (clearly all roots lead to isomorphic fields). We regard $\mathbb{K}_a$ as a "one-parameter family of number fields". We want to consider the average of the prime ideal theorem over this family and, for this purpose, let $\mathcal{A}(X)$ be the set of integers $a \leqslant X$ such that $f(a,y)$ is irreducible. We now define

$$S(X,Y) = \frac{1}{X} \sum_{a\in\mathcal{A}(X)} \sum_{\substack{P\subset\mathcal{O}_a \\ NP\leqslant Y}} \log NP,$$

where the inner sum runs through prime ideals P in the ring of integers $\mathcal{O}_a$ of $\mathbb{K}_a$ and NP is the norm of P. Applying the prime ideal theorem and ignoring error terms, the inner sum is asymptotic to Y so one expects $S(X,Y)$ to be asymptotic to Y under certain conditions on X, Y. We will prove such such estimates in a wider range and with a better error term than that provided by applying the prime ideal theorem for each $\mathbb{K}_a$ individually. We also discuss similar estimates for the Chebotarev density theorem. Finally, we consider the special case of the family of quadratic fields $\mathbb{K}_a = \mathbb{Q}(\sqrt{a})$, which admit stronger bounds.

We remark that out method can also be used (without any substantial losses in the error term) to obtain asymptotic formulas for sums over short intervals, that is, for sums

$$S(X,Y,Z) = \frac{1}{X} \sum_{a\in\mathcal{A}(X,Z)} \sum_{\substack{P\subset\mathcal{O}_a \\ NP\leqslant Y}} \log NP,$$

where $\mathcal{A}(X,Z) = \mathcal{A}(X+Z) \setminus \mathcal{A}(Z)$.

2 Curves as families of number fields

Let $f(x,y)$ be an absolutely irreducible polynomial with integer coefficients. Let γ be the genus of the algebraic curve X defined by $f(x,y)=0$. The Hilbert Irreducibility Theorem (see [11, Sections 9.6, 9.7]) ensures that, for most $a \in \mathbb{Z}$, $f(a,y)$ is irreducible over $\mathbb{Q}$ so we can unambiguously define the number field $\mathbb{K}_a = \mathbb{Q}[y]/(f(a,y))$, for those a with $f(a,y)$ irreducible. Often we can have a more precise version of Hilbert Irreducibility Theorem, by assuming for instance, that X has no positive dimensional linear system of divisors of degree smaller than d and that the Jacobian of X is simple (these conditions are true for all f whose coefficients lie in a Zariski open set of the coefficient space). Under these conditions, the set of a with $f(a, y)$ reducible is finite, since each such a where $f(a, y)$ has a factor of degree $r < d$ gives rise to a rational point in the subvariety of effective divisors of degree r in Jacobian of X and this subvariety has finitely many rational points by the Mordell-Lang conjecture proved by Faltings. Thus in this case we have $\#\mathcal{A}(X) = X + O(1)$. However, for our purposes, it is sufficient to use the bound

$$\#\mathcal{A}(X) = X + O(X^{1/2}), \tag{1}$$

which can be found in [11, Sections 9.6, 9.7] (see also [4, 12] for much more general bounds).

For a given number field K of degree d over $\mathbb{Q}$, the Mordell-Lang conjecture ensures that there are only finitely many values of $a \in Z$ with $\mathbb{K}_a$ isomorphic to K. If one believes Lang's conjecture on varieties of general type, the results of [1] imply a uniform bound independent of K on the number of $a \in Z$ with $\mathbb{K}_a$ isomorphic to K.

3 The prime ideal theorem

It is natural to expect that the error term in our results depend on our knowledge of the distribution of rational primes. Accordingly we define

$$E(Y) = \left| Y - \sum_{p \leqslant Y} \log p \right|$$

where the sum is taken over all rational primes $p \leqslant Y$.

Theorem 1. *Let $f(x, y)$ be an absolutely irreducible polynomial with integer coefficients. Then*

$$S(X, Y) = Y + O\left(Y^{1/2} + X^{-1/2}Y + X^{-1}Y^{3/2}(\log Y)^3 + E(Y) + \log X\right),$$

where the implied constant depends only on f.

Proof. The primes P for which the norm is not a prime divide a rational prime $p \leqslant \sqrt{Y}$ so these primes contribute $O(XY^{1/2})$ to the sum $XS(X, Y)$. We therefore need to consider only split primes.

Let $\Delta(x)$ be the discriminant in y of $f(x, y)$. The contribution of the primes $P|\Delta(a)$ to the inner sum is $O(\log |\Delta(a)|) = O(\log a)$ so those primes contribute $O(X \log X)$ to to $XS(X, Y)$.

It remains to estimate the contribution of the split primes P which do not divide $\Delta(a)$. The number of such primes above a rational prime p is the number of solutions to $f(a,y) \equiv 0 \pmod p$ in $\mathbb{F}_p$. Thus we obtain

$$XS(X,Y) = \sum_{a\in\mathcal{A}(X)} \sum_{p\leqslant Y} \#\{1 \leqslant y \leqslant p \mid f(a,y) \equiv 0 \pmod p\} \log p \\ + O(XY^{1/2} + X\log X). \tag{2}$$

where the condition that $p \nmid \Delta(a)$ is ignored since those can be incorporated in the error term given by argument in the previous paragraph.

Using (1) we see that the conditions $a \in \mathcal{A}(X)$ can be dropped in (2) at the cost of the error term $O(X^{1/2}Y \log X)$. Therefore

$$XS(X,Y) = \sum_{1\leqslant a\leqslant X} \sum_{p\leqslant Y} \#\{1 \leqslant y \leqslant p \mid f(a,y) \equiv 0 \pmod p\} \log p \\ + O(XY^{1/2} + X^{1/2}Y + X\log X). \tag{3}$$

We can now proceed to estimate this sum by interchanging the order of summation and estimate, for a fixed p, the number of solutions of $f(a,y) \equiv 0 \pmod p$, $1 \leqslant a \leqslant X, 1 \leqslant y \leqslant p$. The Weil estimate (see [3] or [10, Chapter III]), gives that the number of solutions of $f(x,y) = 0, x, y \in \mathbb{F}_p$ is $p + O(p^{1/2})$ if f is absolutely irreducible modulo p which, by the Ostrowski theorem, (see [10, Chapter V]), is true for all but finitely many p. Thus we can estimate the number of solutions of

$$f(a,y) \equiv 0 \pmod p, \qquad 1 \leqslant a \leqslant \lfloor X/p \rfloor p,\ 1 \leqslant y \leqslant p,$$

as $\lfloor X/p \rfloor (p + O(p^{1/2}))$.

The number of solutions of

$$f(a,y) \equiv 0 \pmod p, \qquad \lfloor X/p \rfloor p \leqslant a \leqslant X,\ 1 \leqslant y \leqslant p,$$

can be estimated as $\{X/p\}p + O(p^{1/2}(\log p)^2)$ by combining a standard technique with Bombieri's bound [2] for exponential sums along curves (see, for example, [6]).

The two terms combine to give an estimate

$$\begin{aligned}
\sum_{1\leqslant a\leqslant X}\sum_{p\leqslant Y}&\#\{1\leqslant y\leqslant p \mid f(a,y)\equiv 0 \pmod p\}\log p\\
&= \sum_{p\leqslant Y}\sum_{1\leqslant a\leqslant X}\#\{1\leqslant y\leqslant p \mid f(a,y)\equiv 0 \pmod p\}\log p\\
&= \sum_{p\leqslant Y}\left(X\log p + O(Xp^{-1/2}\log p + p^{1/2}(\log p)^3)\right)\\
&= X\sum_{p\leqslant Y}\log p + O\left(XY^{1/2}\log Y + Y^{1/2}(\log Y)^3)\right)\\
&= XY + O\left(XY^{1/2}\log Y + Y^{3/2}(\log Y)^3) + XE(Y)\right).
\end{aligned}$$

Combining this with (3) we obtain

$$\begin{aligned}
S(X,Y) = Y + O(Y^{1/2} &+ X^{-1/2}Y\\
&+ X^{-1}Y^{3/2}(\log Y)^3 + E(Y) + \log X).
\end{aligned} \tag{4}$$

It remains to notice that

$$\max\{Y^{1/2}, X^{-1}Y^{3/2}\} \geqslant \sqrt{Y^{1/2}X^{-1}Y^{3/2}} = X^{-1/2}Y$$

thus the term $X^{-1/2}Y$ in (4) never dominates and can be dropped, which produces the desired result. □

Remark 1. *Clearly Theorem 1 is nontrivial if $X \geqslant Y^{1/2+\varepsilon}$ for some fixed $\varepsilon > 0$.*

Remark 2. *Although current unconditional estimates for $E(Y)$ are far from the expect order of magnitude of $Y^{1/2+o(1)}$ implied by the Riemann Hypothesis, see [8, Corollary 8.30] the corresponding estimates for number fields are even weaker and less uniform. For example, they depend quite badly with respect to the discriminant of the field, see [5], so can only produce estimates similar to the theorem for very small values of X. If we assume the Riemann Hypothesis for $\mathbb{Q}$ only we get a good estimate for $E(Y)$ and thus for $S(X,Y)$ which is much better again than that obtainable by applying the prime ideal theorem to all $\mathbb{K}_a$. Under the much stronger Generalized Riemann Hypothesis, better bounds on the distribution of prime ideals are available, see [9]), which still leads to a weaker error term $O(Y^{1/2}\log X)$.*

4 The Chebotarev density theorem

Let $f(x,y)$ be an absolutely irreducible polynomial with integer coefficients and let $d = \deg_y f$. Let also g be the genus of the algebraic curve $\mathcal{X}$ defined by $f(x,y)=0$. Assume that the cover $\phi : \mathcal{X} \to \mathbb{P}^1$ given by projection onto the x-axis is Galois with Galois group G. Then, for most $a \in \mathbb{Z}$, the extension $\mathbb{K}_a/\mathbb{Q}$ is also Galois with Galois group G. For such a, given an unramified prime ideal P of $\mathbb{K}_a/\mathbb{Q}$, we have its Artin symbol $(\mathbb{K}_a/\mathbb{Q}|P)$ which is an element of G. Its conjugacy class depends only on the rational prime p below P and we denote it by $[\mathbb{K}_a/\mathbb{Q}|p]$.

Theorem 2. *Let $f(x,y)$ be an absolutely irreducible polynomial with integer coefficients and let $\mathcal{X}$ be the algebraic curve defined by $f(x,y)=0$. Assume that the cover $\phi : \mathcal{X} \to \mathbb{P}^1$ given by projection onto the x-axis is Galois with Galois group G. Given a conjugacy class C of G we have*

$$\sum_{a \in \mathcal{A}(X)} \sum_{\substack{p \leqslant Y \\ [\mathbb{K}_a/\mathbb{Q}|p]=C}} \log p$$
$$= |C|XY/|G| + O(XY^{1/2} + X\log X + Y^{3/2}(\log Y)^3 + XE(Y)),$$

where the inner sum runs through rational primes and the implied constant depends only on f.

Proof. As in the proof of the previous theorem, a prime P of $\mathbb{K}_a$ above a rational prime p corresponds to an irreducible factor h of $f(a,y)$ modulo p, except for a few P and a that can be incorporated in the error term. The element $g = (\mathbb{K}_a/\mathbb{Q}|P) \in G$ can be described as the element such that $g(a,\beta) = (a,\beta^p)$ where β is a root of h. The point (a,β) gives an $\mathbb{F}_p$ rational point on the curve $\mathcal{X}^{(g)}$ obtained by twisting $\mathcal{X}$ by g (as in, for example, [3]). Note that these curves are all defined over $\mathbb{F}_p$ (and depend on p, although we omit that from the notation) and are isomorphic to $\mathcal{X}$ over the algebraic closure of $\mathbb{F}_p$ and all have a map $\phi^{(g)} : \mathcal{X}^{(g)} \to \mathbb{P}^1$ of the same degree as ϕ, since ϕ is G-invariant by hypothesis. So if there is a point v in $\mathcal{X}^{(g)}(\mathbb{F}_p)$, $\phi^{(g)}(v) = a$, then there are $|G|$ such points, except for the $O(1)$ values of a over which $\phi^{(g)}$ is ramified. Thus, to estimate the sum in the theorem, it is enough to estimate,

$$\sum_{p \leqslant Y} \sum_{g \in C} \sum_{1 \leqslant a \leqslant X} \#\{v \in \mathcal{X}^{(g)}(\mathbb{F}_p) \mid \phi^{(g)}(v) = a\} \log p/|G|.$$

To estimate the terms of this sum, again we can break up the interval $1 \leqslant a \leqslant X$ into $1 \leqslant a \leqslant [X/p]p$ and $[X/p]p \leqslant a \leqslant X$, and use the Weil estimate, in the former and the estimate of [6] in the latter. Note that the estimate of [6] depends on the degree and dimension of a fixed projective embedding of $\mathcal{X}^{(g)}$ in addition to the degree of $\phi^{(g)}$, but these curves have all the same genus and a curve of genus γ over a finite field can always be embedded in a projective space with degree and dimension $O(\gamma+1)$. We get

$$\#\{v \in \mathcal{X}^{(g)}(\mathbb{F}_p) \mid \phi^{(g)}(v) = a\} = X + O(p^{1/2}(\log p)^2 + Xp^{-1/2})$$

and the proof follows just as in the previous theorem. □

Remark 3. *Clearly Theorem 2 is nontrivial if* $X \geqslant Y^{1/2+\varepsilon}$ *for some fixed* $\varepsilon > 0$.

5 A special case

In the special case of the polynomial $f(x,y) = x - y^2$, that is, in the case of $\mathbb{K}_a = \mathbb{Q}(\sqrt{a})$, instead of the Weil and Bombieri bounds, one can simply apply the Burgess bound on the number of quadratic residues in an interval, see [8, Theorem 12.6] and thus obtain an asymptotic formula for $S(X,Y)$ in a wider range of X and Y compared to that of Theorem 1.

Furthermore, we note that the proof of Theorem 1 does not take any advantage of averaging over p and each inner sum over a is estimated "individually". However for $f(x,y) = x - y^2$, using the Heath-Brown [7] large sieve inequality for real characters, allows us to use the averaging over p in a substantial way, and extend the range on nontriviality even further.

Theorem 3. *Let* $f(x,y) = x - y^2$. *Then*

$$S(X,Y) = Y + O\left(X^{o(1)}Y^{1/2} + X^{-1/2}Y^{1+o(1)} + E(Y)\right),$$

where the implied constant is absolute.

Proof. We proceed as in the proof of Theorem 1, however we estimate the sum in (3) slightly differently. Now, using the Legendre symbol (a/p) to express the number of solutions to a quadratic congruence, we write

$$\begin{aligned}
&\sum_{1\leqslant a\leqslant X}\sum_{p\leqslant Y}\#\{1\leqslant y\leqslant p \mid a\equiv y^2 \pmod p\}\log p\\
&\qquad=\sum_{p\leqslant Y}\sum_{1\leqslant a\leqslant X}\#\{1\leqslant y\leqslant p \mid a\equiv y^2 \pmod p\}\log p\\
&\qquad=\sum_{p\leqslant Y}\sum_{1\leqslant a\leqslant X}\left(1+\left(\frac{a}{p}\right)\right)\log p\\
&\qquad=X\sum_{p\leqslant Y}\log p+\sum_{p\leqslant Y}\sum_{1\leqslant a\leqslant X}\left(\frac{a}{p}\right)\log p.
\end{aligned}$$

Combining this with (3) we obtain

$$S(X,Y)=Y+O\left(Y^{1/2}+X^{-1/2}Y+\log X+E(Y)+R(X,Y)\log Y\right), \quad (5)$$

where

$$R(X,Y)=X^{-1}\sum_{p\leqslant Y}\left|\sum_{1\leqslant a\leqslant X}\left(\frac{a}{p}\right)\right|.$$

By the result of Heath-Brown [7], for any complex-valued function $f(a)$,

$$\sum_{p\leqslant Y}\left|\sum_{1\leqslant a\leqslant X}f(a)\left(\frac{a}{p}\right)\right|^2\leqslant (XY)^{o(1)}(X+Y)\sum_{1\leqslant a\leqslant X}|f(a)|^2$$

(in fact the result is more general and the external summation can be extended to square-free integers $s\leqslant Y$). Thus, applying this bound with $f(a)=1$, by the Cauchy inequality, we obtain

$$\begin{aligned}
R(X,Y) &\leqslant X^{-1}\left(\pi(Y)\sum_{p\leqslant Y}\left|\sum_{1\leqslant a\leqslant X}\left(\frac{a}{p}\right)\right|^2\right)^{1/2}\\
&\leqslant X^{-1}\left((XY)^{1+o(1)}(X+Y)\right)^{1/2}\leqslant X^{o(1)}Y^{1/2}+X^{-1/2+o(1)}Y^{1+o(1)}.
\end{aligned}$$

Substituting this estimate in (5), and discarding the terms which never dominate, we obtain the desired result. □

Remark 4. *Clearly Theorem 3 is nontrivial if $X\geqslant Y^{\varepsilon}$ for some fixed $\varepsilon>0$.*

References

[1] D. Abramovich and J. F. Voloch, 'Lang's conjecture, fibered powers and uniformity', *New York Journal of Math.*, **2** (1996), 20–34.

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

[3] E. Bombieri, 'Counting points on curves over finite fields (d'aprés S. A. Stepanov)'. *Séminaire Bourbaki, 25éme année (1972/1973), Exp. No. 430*, Lecture Notes in Math., Vol. 383, Springer, Berlin, 1974, 234–241.

[4] S. D. Cohen, 'The distribution of Galois groups and Hilbert's irreducibility theorem', *Proc. London Math. Soc.*, **43** (1981), 227–250.

[5] L. J. Goldstein, 'A generalization of the Siegel-Walfisz theorem', *Trans. Amer. Math. Soc.*, **149** (1970), 417–429.

[6] A. Granville, I. E. Shparlinski and A. Zaharescu, 'On the distribution of rational functions along a curve over $\mathbb{F}_p$ and residue races', *J. Number Theory*, **112** (2005), 216–237.

[7] D. R. Heath-Brown, 'A mean value estimate for real character sums', *Acta Arith.*, **72** (1995), 235–275.

[8] H. Iwaniec and E. Kowalski, *Analytic number theory*, Amer. Math. Soc., Providence, RI, 2004.

[9] J. C. Lagarias and A. M. Odlyzko, 'Effective versions of the Chebotarev density theorem', *Algebraic number fields: L-functions and Galois properties (Proc. Sympos., Univ. Durham, Durham, 1975)*, Academic Press, London, 1977, 409–464.

[10] W. M. Schmidt, *Equations over finite fields: An elementary approach*, Lecture Notes in Math., Vol. 536, Springer, Berlin, 1976.

[11] J. P. Serre, *Lectures on the Mordell-Weil theorem*, Vieweg, 1997.

[12] U. Zannier, 'On the number of times a root of $f(n,x)=0$ generates a field containing a given number field', *J. Number Theory*, **72** (1998), 1–12.