Math. Res. Lett.
Volume 24, Number 3, 679–687, 2017

Remarks on the error term in Chebotarev's density theorem

Joël Bellaïche

We answer a question of Murty, Murty and Saradha on the best possible error term in Chebotarev's density theorem, and a question of Serre on the first prime having a specified Frobenius in a given extension.

1. The error term in Chebotarev's density theorem

In [8], and then again, without the third author, in [9], Ram Murty, Kumar Murty and Saradha prove a result (conditional to some standard conjectures of analytic number theory, namely the General Riemann Hypothesis and the Artin's conjecture) bounding the error term in Chebotarev's Density Theorem (see (3) below) and ask whether an improved bound (see (5) below) holds. The aim of this article is to prove that the answer to this question is negative, to answer (by the affirmative) a related question of Serre from [11], and more generally, to discuss the best possible error terms (of the forms considered in [8] and [9]) in Chebotarev's density theorem.

To formalize this question of Ram Murty, Kumar Murty and Saradha precisely, let us fix some notations: in all this paper, L will denote a finite Galois extension of $\mathbb{Q}$ of degree n and Galois group G, and D will denote a conjugacy set (that is, a union of conjugacy classes) in G. We will denote by M the product of all prime numbers that are ramified in L. For x a positive real number, we call $\pi_D(x)$ the number of primes $p < x$ such that the conjugacy class $\mathrm{Frob}_{p,L/\mathbb{Q}}$ of G is contained in D. By (GRH) we shall mean as in [8] the Generalized Riemann Hypothesis for all Artin L-functions.

The first effective version of Chebotarev's density theorem, proved by Lagarias and Odlyzko ([5]) and soon thereafter improved by Serre ([11, (20_R),

page 134]) states[1], that, assuming (GRH):

$$(1) \qquad \pi_D(x) = \frac{|D|}{|G|}\mathrm{Li}\,(x) + O\left(x^{1/2}|D|(\log x + \log|G| + \log M)\right).$$

The implied constant in the above formula is absolute. In this paper we shall not be interested in the logarithmic terms in x and $|G|$. Therefore, let us replace (1) by its following slight weakening:

$$(2) \qquad \text{For every } \epsilon > 0, \quad \pi_D(x) = \frac{|D|}{|G|}\mathrm{Li}\,(x) + O\left(x^{1/2+\epsilon}|D||G|^{\epsilon}\log M\right).$$

In this formula the implied constant depends only on ϵ.

Later, Murty, Murty and Saradha proved (cf. [8, Corollary 3.7]), using (GRH) and the Artin's conjecture of holomorphy of Artin L-functions, that

$$(3) \qquad \pi_D(x) = \frac{|D|}{|G|}\mathrm{Li}\,(x) + O\left(x^{1/2}|D|^{1/2}(\log x + \log|G| + \log M)\right)$$

with an absolute implied constant, which again can be slightly weakened into:

$$(4) \qquad \text{For every } \epsilon > 0, \quad \pi_D(x) = \frac{|D|}{|G|}\mathrm{Li}\,(x) + O\left(x^{1/2+\epsilon}|D|^{1/2}|G|^{\epsilon}\log M\right)$$

In the same paper [8, §3.13] (and also in [9] without the third author), Murty, Murty and Saradha ask the following question. Let $\alpha(G)$ be the

[1] Let us precise a point of terminology relative to our use of Landau's O notation in this statements and other in this paper. Let I be a fixed interval of $\mathbb{R}_+$ not bounded above. In all this article, one will take $I = [2, \infty($. Let P, Q be two sets of parameters, and let f, g be two real-valued functions on $P \times Q \times I$. We assume that g takes only positive values. Let $r : P \times Q \to I$ be another function. We shall often write sentences of the type *for $x \geq r(p,q)$, one has $f(p,q,x) = O(g(p,q,x))$, the implied constant depending only on p*. The formal meaning of this sentence is:

$$\forall p \in P, \exists C > 0, \forall q \in Q, \forall x \in I, \quad x \geq r(p,q) \Rightarrow |f(p,q,x)| \leq Cg(p,q,x).$$

When no range is precised, that is when the phrase *for $x > r(p,q)$* is ommited, the meaning will be:

$$\forall p \in P, \exists C > 0, \forall q \in Q, \forall x \in I, \quad |f(p,q,x)| \leq Cg(p,q,x).$$

This interpretation of O is the most frequently used nowadays (for example, in [4], cf. *loc. cit.* page 7). However, as pointed to us by Serre, this is not Landau's original meaning, nor Bourbaki's.

number of conjugacy classes in G. Is it true that (with an absolute implied constant)

(5)
$$\pi_D(x) = \frac{|D|}{|G|}\mathrm{Li}\,(x) + O\left(x^{1/2+\epsilon}|D|^{1/2}\alpha(G)^{-1/2}(\log x + \log|G| + \log M)\right) ?$$

Once again, a positive answer to this question would mean a positive answer to its following simplified version. Is it true that (with an implied constant depending only on ϵ)

(6) For every $\epsilon > 0$, $$\pi_D(x) = \frac{|D|}{|G|}\mathrm{Li}\,(x) + O\left(x^{1/2+\epsilon}|D|^{1/2}\alpha(G)^{-1/2}|G|^{\epsilon}\log M\right) ?$$

Here the implied constant depends only on ϵ.

The answer to (5) and (6) is no for a trivial reason: *there is no specified range*. Indeed, assume that $|D| = 1$ to fix ideas, and that M is constant. If $x < \alpha(G)^c$ for some constant $c < 1$, then the error term in those formulas goes to 0 when $\alpha(G)$ goes to infinity, hence $\pi_D(x+1) - \pi_D(x)$ goes to 0 when x and $\alpha(G)$ go to infinity with $x < \alpha(G)^c$. So, for $\alpha(G)$ large enough and $x < \alpha(G)^c$, $\pi_D(x+1) = \pi_D(x)$ since those numbers are integers. Now, choose a field $L/\mathbb{Q}$ unramified outside M, with Galois group G such that $\alpha(G)$ is large enough in the preceding sense (of course there are plenty of such field even among cyclotomic fields) and take $D = \{\mathrm{Frob}_p\}$ for a prime $p < \alpha(G)^c$. Then clearly $\pi_D(p+1) = \pi_D(p) + 1$, a contradiction.

We note that this omission of the range made in [8] and in [9] seems quite frequent in similar questions in the literature of analytic number theory, for example those concerning the primes in an arithmetic progression with common difference q: cf. [7, First paragraph of page 309] or [4, (17.5)], which are both false as stated for the same trivial reason. However, the remaining of the discussion in [4, §17.1] makes clear that the restriction $x > q$ is implicitly assumed, and it is likely that such a restriction was also in the authors' minds in [7].

Similarly, it is natural in the questions (5) and (6) to restrict our attention to the range $x \geq |G|$ or even, to be more prudent, to $x \geq |G|\log^{\alpha}|G|$ for every $\alpha > 0$. That is to say, one is led to ask:

(7) For every $\epsilon > 0$, is it true that if $x > |G|$,
$$\pi_D(x) = \tfrac{|D|}{|G|}\mathrm{Li}\,(x) + O\left(x^{1/2+\epsilon}|D|^{1/2}\alpha(G)^{-1/2}|G|^{\epsilon}\log M\right),$$
the implied constant depending only on ϵ?

And:

$$\text{For every } \epsilon > 0 \text{ and every } \alpha > 0, \text{ is it true that if } x > |G|(\log|G|)^{\alpha},$$
$$\pi_D(x) = \frac{|D|}{|G|}\mathrm{Li}\,(x) + O\left(x^{1/2+\epsilon}|D|^{1/2}\alpha(G)^{-1/2}|G|^{\epsilon}\log M\right), \tag{8}$$
$$\text{the implied constant depending only on } \epsilon \text{ and } \alpha?$$

Remark 1. Consider the cyclotomic case $L = \mathbb{Q}(\mu_q)$ (so $G = (\mathbb{Z}/q\mathbb{Z})^*$) and $D = \{d\}$, where q and d are relatively prime positive integers. In this case, $\pi_D(x)$ counts the primes $p < x$ such that $p \equiv d \pmod q$, and a conjecture of Friedlander and Granville ([3, Conjecture 1(b), page 366]), correcting the famous conjecture of Montgomery ([6], [7]), states

$$\text{For every } \epsilon > 0, \text{ if } x > q,$$
$$\pi_D(x) = \frac{1}{\phi(q)}\mathrm{Li}\,(x) + O\left(x^{1/2+\epsilon}q^{-1/2}\right), \tag{9}$$

Using the well-known estimate $q/\log\log q < \phi(q) < q$, it is an easy exercise to see that, in this cyclotomic case with $|D| = 1$, (9) $\Longrightarrow$ (8). At any rate it is plain that (7) and (8) *in the cyclotomic case with* $|D| = 1$ on the one hand, and (9) on the other hand are very close, and it is almost certain that those three conjectures hold or fall together.

Back to general case, our main result is that, even if we add the forgotten restriction of the range, the answer to Murty, Murty, and Saradha's question is no.

Theorem 1. *The answer to (8), hence to (7), is no.*

We will prove this theorem twice, by giving two separate counter-examples: one in the case G dihedral, $D = \{1\}$ (see Proposition 1), the second in the case G abelian, $|D|$ large (see Proposition 2). The fact that two natural generalizations of the conjecture of Friedlander and Granville fail suggest that this conjecture is either extremely difficult (which of course, was clear to begin with), or even, possibly, false.

Let us now discuss the question of Serre. A result of Lagarias and Odlyzko ([5]) states that, under (GRH), $\pi_D(x) > 0$ if $x > c(\log d_K)^2$, where c is some absolute constant. Serre asks ([11, Remark 2, page 135]) whether the exponent 2 in this formula is the best possible. In view of [11, Proposition 6],

which in our notations states

$$|G|\log M/2 \leq \log d_K \leq (|G|-1)\log M + |G|\log|G|,$$

the question is equivalent to:

$$\begin{gathered}\text{Does there exist } e<2 \text{ and } c>0,\\ \text{such that } x > c|G|^e \log M \text{ implies } \pi_D(x)>0?\end{gathered} \tag{10}$$

We shall see (cf. Prop. 1) that the answer to (10) is no — that is, the answer to Serre's question "is 2 the best possible constant?" is yes.

On a more constructive tone, one may then ask: what is the best possible error term in Chebotarev's density theorem? Of course, in this generality, the question is not interesting (the answer is obviously $|\pi_D(x) - \frac{|D|}{|G|}\mathrm{Li}\,(x)|$): we need to restrict our study to some special families of allowed error terms, for example error terms depending only on the size of the group G and the set D through the product of a power of $|G|$ and a power of $|D|$.

Theorem 2. *For two real numbers a and b, consider the following assertion:*

$$\begin{gathered}\textit{For every } \epsilon,\alpha>0, \textit{ in the range } x>|G|(\log|G|)^\alpha,\\ \pi_D(x) = \tfrac{|D|}{|G|}Li\,(x) + O\left(x^{1/2+\epsilon}|D|^a|G|^{b+\epsilon}\log M\right)\\ \textit{with an implied constant depending only on } a,\ b,\ \epsilon \textit{ and } \alpha.\end{gathered} \tag{$C_{a,b}$}$$

Then for $(C_{a,b})$ to be true it is necessary, and, under (GRH) and Artin, sufficient that $b\geq 0$ and $a+b\geq 1/2$.

In other words, the estimate of Ram Murty, Kumar Murty and Saradha (4), or $(C_{1/2,0})$ in our language, is the best possible among estimates of the form $(C_{a,b})$. Indeed, if $a+b\geq 1/2$, and $b\geq 0$, $|D|^{1/2}\leq |D|^{a+b} = |D|^a|D|^b \leq |D|^a|G|^b$ because $|D|<|G|$, and $(C_{1/2,0})$ implies $(C_{a,b})$, hence the sufficiency in the above theorem. The necessity will be proved in Prop. 1 and Prop. 2.

One may then ask for other types of error estimates. For example, question (6) suggests that we look at error terms of the form

$$O\left(x^{1/2+\epsilon}|D|^a\alpha(G)^b|G|^\epsilon\log M\right).$$

Theorem 3. *For two real numbers a and b, consider the following assertion:*

$$(C'_{a,b}) \qquad \begin{array}{c} \text{For every } \epsilon > 0,\ \alpha > 0, \text{ in the range } x > |G|(\log|G|)^{\alpha}, \\ \pi_D(x) = \frac{|D|}{|G|} Li(x) + O\left(x^{1/2+\epsilon}|D|^a \alpha(G)^b |G|^{\epsilon} \log M\right) \\ \text{with an implied constant depending only on } a,\ b,\ \epsilon \text{ and } \alpha. \end{array}$$

Then for $(C'_{a,b})$ to be true it is necessary that $b \geq 0$ and $a + b \geq 1/2$.

In this case, since $\alpha(G)$ may be larger or smaller than $|D|$, it is not clear in this case that $(C'_{1/2,0})$ (which is the same as $(C_{1/2,0})$, hence a theorem under (GRH) and Artin) implies $(C'_{a,b})$ if $b \geq 0$, $a + b \geq 1/2$. That is to say, we ignore (even under (GRH) and Artin) if $(C'_{a,b})$ is true for some $b > 0$, $a + b = 1/2$, for example for $a = 1/4$, $b = 1/4$. This would be very surprising however, as it would mean a better bound, for the same $|G|$ and $|D|$, in the non-abelian case than in the abelian case, and at any rate contrary to the intuition underlying Question (6) where $\alpha(G)$ appeared with a negative exponent b, hence giving a better bound in the abelian than in the non-abelian case.

Let us end this already too long introduction that we can get better and useful estimate for the error term which make intervene the fine *structure* of the group G and the set D rather than just their size $|G|$ and $|D|$ or the number $\alpha(G)$ of conjugacy classes of G. See [4, page 143] and [1].

2. A family of dihedral examples with $D = \{1\}$

The examples will depend on an integral parameter $n = 2^r$ with $r \geq 2$. Let $\mathcal{O}$ be the order $\mathbb{Z}[\sqrt{-n^2}] = \mathbb{Z}[ni]$ in the field of Gaussian numbers $\mathbb{Q}(i)$. Let L be the ring class field of $\mathcal{O}$. As usual let $G = \mathrm{Gal}(L/\mathbb{Q})$, M the product of all primes ramified in L. We set $D = \{1\}$, so $\pi_D(x)$ counts the primes less than x that are totally split in L.

Proposition 1. *For L, D as above and $n = |G|$ large enough, $(C_{a,b})$ and $(C'_{a,b})$ are false whenever $b < 0$. Moreover (10) is false whenever $e < 2$.*

We collect in the following lemma various elementary results, mainly from Cox's book.

Lemma 1.

(i) $M = 2$

(ii) *G is a dihedral group of order n.*

(iii) *If $x = |G|^2 = n^2$, then $\pi_D(x) = 0$.*

(iv) $\alpha(G) > n/4$.

Proof. The conductor $f = [\mathbb{Z}[i] : \mathcal{O}]$ of the order $\mathcal{O}$ is n, hence the class number of that order is $h(\mathcal{O}) = \frac{f}{[\mathbb{Z}[i]^* : \mathcal{O}^*]} = \frac{f}{2} = n/2 = 2^{r-1}$ according to [2, Theorem 7.24]. Hence by definition of the ring class field and by class field theory, L is an abelian extension of $\mathbb{Q}(i)$ of degree $n/2$, ramified only at (the prime dividing) 2. Therefore, G is dihedral of order n, and $M = 2$. This proves (i) and (ii).

By [2, Theorem 9.4], an odd prime p is totally split in L if and only if it is represented by the form

$$a^2 + n^2 b^2.$$

It is clear that no prime $p \leq n^2$ is of this form, hence $\pi_D(x) = 0$ if $x = n^2$, which is (iii).

Finally (iv) follows from the computation of the number of conjugacy classes in a dihedral group, which is easy and standard (see e.g. [10, §5.3]) □

Now assume that formula $(C_{a,b})$ or $(C'_{a,b})$ is true in the case under consideration for some value of the parameters a and b such that $b < 0$. We are going to obtain a contradiction. Since $\alpha(G) < |G|$, it suffices to consider the case of $(C'_{a,b})$:

$$\pi_D(x) = \frac{1}{n}\mathrm{Li}\,(x) + O(x^{1/2+\epsilon}\alpha(G)^b n^\epsilon).$$

By Lemma 1(iv), $\alpha(G)^b = O(n^b)$, hence

$$\pi_D(x) = \frac{1}{n}\mathrm{Li}\,(x) + O(x^{1/2+\epsilon} n^{b+\epsilon}).$$

Let us fix some $\alpha > 0$. If n is large enough, $x = n^2$ is certainly in the range $x > n\log(n)^\alpha$, so $\pi_D(x) = 0$, and the formula becomes $\frac{1}{n}\mathrm{Li}\,(n^2) = O(n^{1+b+3\epsilon})$ or $\mathrm{Li}\,(n^2) = O(n^{2+b+3\epsilon})$. Since $b < 0$, we can choose $\epsilon > 0$ such that $-\epsilon' := b + 3\epsilon < 0$, and we get $\mathrm{Li}\,(n^2) = O(n^{2-\epsilon'})$, which is absurd since $\mathrm{Li}\,(n^2) \sim n^2/(2\log n)$. This completes the proof of the first part of Proposition 1.

Concerning Serre's question (10), one has just seen that $\pi_D(x) = 0$ for all $x \leq |G|^2 = \frac{1}{\log 2}|G|^2 \log M$, which shows that (10) cannot be true for $e < 2$. This completes the proof.

3. A family of abelian examples with $|D|$ large

Again, the example will depend on a integral parameter $n = 2^r$ with $r \geq 2$. We define $L = \mathbb{Q}(\mu_{2^{r+1}}) = \mathbb{Q}(\mu(2n))$, so that $G = \mathrm{Gal}(L/\mathbb{Q}) = (\mathbb{Z}/2n\mathbb{Z})^*$ has order n, and for an odd prime p, $\mathrm{Frob}_{p,L/\mathbb{Q}}$ is just $p \pmod{2n}$. One also have $M = 2$, and $\alpha(G) = |G| = n$. Fix an $\alpha > 0$, such that $\alpha < 1$. We let $D \subset (\mathbb{Z}/2n\mathbb{Z})^*$ be the set of all odd residue classes d modulo $2n$ such that the arithmetic progression $d + 2n\mathbb{Z}$ does not contain any prime smaller than $n \log(n)^\alpha$. Clearly, the complement of D has size at most $\pi(n \log(n)^\alpha) = o(n)$ by the prime number theorem, so $|D| \sim n$ when n goes to infinity. On the other hand, by definition $\pi_D(n \log(n)^\alpha) = 0$.

Proposition 2. *For L, D as above and $n = |G|$ large enough, $(C_{a,b})$ and $(C'_{a,b})$ are false if $a + b < 1/2$*

Indeed, $(C_{a,b})$ and $(C'_{a,b})$ are identical in this case, and state that for $x \geq n \log(n)^\alpha$,

$$\pi_D(x) = \frac{|D|}{n} \mathrm{Li}\,(x) + O\left(x^{1/2+\epsilon} n^{a+b+\epsilon}\right).$$

Applying this to $x = n \log(n)^\alpha$, we get, since $\pi_D(x) = 0$,

$$\frac{|D|}{n} \mathrm{Li}\,(x) = O(n^{a+b+1/2+2\epsilon} \log(n)^{\alpha(1/2+\epsilon)})$$

which implies since $|D| \sim n$, and $n \leq x$,

$$n = O(n^{a+b+1/2+2\epsilon} \log(n)^\beta)$$

where β is some real number depending only on ϵ and α. If $a + b < 1/2$, one can choose $\epsilon > 0$ such that the exponent of n in the RHS is < 1, giving a contradiction.

References

[1] J. Bellaïche, *Théorème de Chebotarev et complexité de Littlewood*, Ann. Sci. Éc. Norm. Supér. (4) **49** (2016), no. 3, 579–632.

[2] D. Cox, *Primes of the form $x^2 + ny^2$. Fermat, class field theory and complex multiplication*, John Wiley & Sons, Inc., New York, 1989.

[3] J. Friedlander and A. Granville, *Limitations to the equi-distribution of primes. I*, Ann. of Math. (2) **129** (1989), no. 2, 363–382.

[4] H. Iwaniec and E. Kowalski, *Analytic number theory*, AMS Colloquium publication **53** (2004).

[5] 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), pp. 409–464, Academic Press, London, 1977.

[6] H. Montgomery, *Topics in multiplicative number theory*, Lecture Notes in Mathematics, Vol. 227. Springer-Verlag, Berlin-New York, 1971, ix+178pp.

[7] H. Montgomery, *Problems concerning prime numbers*, Mathematical developments arising from Hilbert problems (Proc. Sympos. Pure Math., Northern Illinois Univ., De Kalb, Ill., 1974), pp. 307–310, Proc. Sympos. Pure Math., Vol. XXVIII, Amer. Math. Soc., Providence, R.I., 1976.

[8] M. Ram Murty, V. Kumar Murty, and N. Saradha, *Modular forms and the Chebotarev density theorem*, American Journal of Mathematics **110** (Apr., 1988), no. 2, 253–281.

[9] M. Ram Murty and V. Kumar Murty, *Non-vanishing of L-functions and applications*, Progress in Mathematics **157**, Birkhäuser Verlag, Basel, 1997

[10] J.-P. Serre, *Représentations linéaires des groupes finis*, Hermann, Paris, 1974.

[11] J.-P. Serre, *Quelques applications du théorème de densité de Chebotarev*, Inst. Hautes Études Sci. Publ. Math. **54** (1981), 323–401.

Department of Mathematics, Brandeis University
415 South Street, Waltham, MA 02454-9110, USA
E-mail address: jbellaic@brandeis.edu

Received October 24, 2012