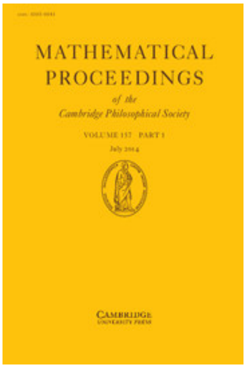
Mathematical Proceedings of the Cambridge Philosophical Society

http://journals.cambridge.org/PSP



MATHEMATICAL
PROCEEDINGS
of the
Cambridge Philosophical Society
VOLUME 157 PART 1
July 2014

CAMBRIDGE
UNIVERSITY PRESS

Artin's primitive root conjecture and a problem of Rohrlich

CHRISTOPHER AMBROSE

Mathematical Proceedings of the Cambridge Philosophical Society / Volume 157 / Issue 01 / July 2014, pp 79 - 99
DOI: 10.1017/S0305004114000206, Published online: 01 May 2014

Link to this article: http://journals.cambridge.org/abstract_S0305004114000206

How to cite this article:
CHRISTOPHER AMBROSE (2014). Artin's primitive root conjecture and a problem of Rohrlich . Mathematical Proceedings of the Cambridge Philosophical Society, 157, pp 79-99 doi:10.1017/S0305004114000206

Math. Proc. Camb. Phil. Soc. (2014), **157**, 79–99 © *Cambridge Philosophical Society* 2014
doi:10.1017/S0305004114000206
First published online 1 May 2014

Artin's primitive root conjecture and a problem of Rohrlich

BY CHRISTOPHER AMBROSE

Mathematisches Institut, Georg-August-Universität Göttingen,
Bunsenstraße 3-5, 37073 *Göttingen, Deutschland.*
e-mail: ambrose@uni-math.gwdg.de

(*Received* 9 *September* 2013; *revised* 5 *February* 2014)

Abstract

Let $\mathbb{K}$ be a number field, Γ a finitely generated subgroup of $\mathbb{K}^*$, for instance the unit group of $\mathbb{K}$, and $\kappa > 0$. For an ideal $\mathfrak{a}$ of $\mathbb{K}$ let $\mathrm{ind}_\Gamma(\mathfrak{a})$ denote the multiplicative index of the reduction of Γ in $(\mathcal{O}_\mathbb{K} / \mathfrak{a})^*$ (whenever it makes sense). For a prime ideal $\mathfrak{p}$ of $\mathbb{K}$ and a positive integer γ let $\mathcal{I}_\gamma^\kappa(\mathfrak{p})$ be the average of $\mathrm{ind}_{\langle a_1,\ldots,a_\gamma\rangle}(\mathfrak{p})^\kappa$ over all tupels $(a_1, \ldots, a_\gamma) \in (\mathcal{O}_\mathbb{K} / \mathfrak{p})^{*\gamma}$. Motivated by a problem of Rohrlich we prove, partly conditionally on fairly standard hypotheses, lower bounds for $\sum_{\mathcal{N}\mathfrak{a}\leqslant x} \mathrm{ind}_\Gamma(\mathfrak{a})^\kappa$ and asymptotic formulae for $\sum_{\mathcal{N}\mathfrak{p}\leqslant x} \mathcal{I}_\gamma^\kappa(\mathfrak{p})$.

1. *Introduction*

Let $\mathbb{K}$ be a number field with ring of integers $\mathcal{O}_\mathbb{K}$ and unit group $\mathcal{U}_\mathbb{K} := \mathcal{O}_\mathbb{K}^*$, an abelian group of rank $r + s - 1$, where r and s denote the number of real and pairs of complex embeddings of $\mathbb{K}$, respectively. For any ideal $\mathfrak{a}$ of $\mathbb{K}$ one may consider the image $\overline{\mathcal{U}_\mathbb{K}}$ of $\mathcal{U}_\mathbb{K}$ in $(\mathcal{O}_\mathbb{K} / \mathfrak{a})^*$ and ask for the behaviour of its residual index, denoted by $\mathrm{ind}_{\mathcal{U}_\mathbb{K}}(\mathfrak{a})$. This quantity behaves rather erratically as $\mathfrak{a}$ runs through ideals of $\mathbb{K}$, if $\mathcal{U}_\mathbb{K}$ is infinite, i.e. $\mathbb{K}$ is neither $\mathbb{Q}$ nor an imaginary quadratic field. In this case a suitable generalisation of Artin's conjecture on primitive roots to number fields (see e.g. [**15**]) suggests that the index should often be small and in fact $\overline{\mathcal{U}_\mathbb{K}}$ should even generate $(\mathcal{O}_\mathbb{K} / \mathfrak{a})^*$ quite frequently. On the other hand, Rohrlich [**25**] has explicitly constructed a (very sparse) infinite family of ideals $\mathfrak{a}$ of $\mathbb{K}$ for which the index is as large as $(\mathcal{N}\mathfrak{a})^{1-\varepsilon}$, where $\mathcal{N}\mathfrak{a}$ denotes the number of elements in $\mathcal{O}_\mathbb{K} / \mathfrak{a}$. This construction was one of the key ingredients for strong bounds towards the Ramanujan conjecture for GL_n over number fields [**19**]. But at the same time the sparseness of this sequence prevented an extension of the Kim–Sarnak bound [**11**] for GL_2 over $\mathbb{Q}$ to general number fields (see [**3**] for more details).

In a recent paper of Rohrlich [**24**] the quantity $\mathrm{ind}_{\mathcal{U}_\mathbb{K}}(\mathfrak{a})$ appeared once again. This time its average order occupied an important position in connection with counting self-dual Artin representations over number fields. In this regard Zelinsky [**31**] has recently proved the upper bound

$$\sum_{\mathcal{N}\mathfrak{a}\leqslant x} \mathrm{ind}_{\mathcal{U}_\mathbb{K}}(\mathfrak{a}) \ll \frac{x^2}{\log^{3-\varepsilon} x} \tag{1·1}$$

for any $\varepsilon > 0$, if $\mathcal{U}_\mathbb{K}$ is infinite, thereby improving the trivial bounds

$$x \ll \sum_{\mathcal{N}\mathfrak{a}\leqslant x} \mathrm{ind}_{\mathcal{U}_\mathbb{K}}(\mathfrak{a}) \ll x^2. \tag{1·2}$$

Apart from this, however, little seems to be known.

In this paper we will establish non-trivial lower bounds for the sum in (1·1) and also prove a conditional result which, somewhat unexpectedly, suggests that the correct order of growth is in fact $x^{2+o(1)}$. These lower bounds will be proven in a more general setting. Instead of the average behaviour of $\mathrm{ind}_{\mathcal{U}_{\mathbb{K}}}(\mathfrak{a})$ we consider arbitrary (positive) moments of the index $\mathrm{ind}_{\Gamma}(\mathfrak{a})$ of the reduction modulo $\mathfrak{a}$ of any (not necessarily torsion-free) subgroup Γ of $\mathbb{K}^*$ of finite rank $\gamma \geqslant 1$ (the case of finite Γ being uninteresting). Clearly we must restrict to those ideals $\mathfrak{a}$ for which the reduction $\overline{\Gamma}$ modulo $\mathfrak{a}$ makes sense and is contained in $(\mathcal{O}_{\mathbb{K}} / \mathfrak{a})^*$. For convenience this property will be denoted by $\overline{\Gamma} \subset (\mathcal{O}_{\mathbb{K}} / \mathfrak{a})^*$.

Another problem addressed by this paper is the average behaviour of $\mathrm{ind}_{\Gamma}(\mathfrak{p})$ over prime ideals $\mathfrak{p}$ of $\mathbb{K}$. The advantage here is that the multiplicative structure of the residue field $\mathcal{O}_{\mathbb{K}} / \mathfrak{p}$ is much easier to handle than the multiplicative structure of $\mathcal{O}_{\mathbb{K}} / \mathfrak{a}$ if $\mathfrak{a}$ is composite. In some sense the averaging over prime ideals therefore seems to be the more natural problem. In [**29**], Wagstaff has provided heuristic arguments for $\mathbb{K} = \mathbb{Q}$ which suggest that the average multiplicative index of an integer $a \neq 0, \pm 1$ modulo p equals a positive multiple of $\log p$, but even under Generalised Riemann Hypothesis (GRH), a rigorous proof seems out of reach (see [**5**] for some unconditional results). More generally, for any real $\kappa > 0$ we expect

$$\sum_{\substack{\mathcal{N}\mathfrak{p} \leqslant x \\ \overline{\Gamma} \subset (\mathcal{O}_{\mathbb{K}} / \mathfrak{p})^*}} \mathrm{ind}_{\Gamma}(\mathfrak{p})^{\kappa} \sim \begin{cases} A_{\Gamma}^{\kappa}\,\mathrm{li}(x), & \text{if } \gamma > \kappa, \\ A_{\Gamma}^{\kappa} x, & \text{if } \gamma = \kappa, \\ A_{\Gamma}^{\kappa}\,\mathrm{li}(x^{\kappa-\gamma+1}), & \text{if } \gamma < \kappa, \end{cases} \tag{1·3}$$

with a positive constant A_{Γ}^{κ} depending on Γ and κ, and $\mathrm{li}(x)$ denoting the logarithmic integral. In this paper we prove results which support this conjecture.

2. *Statements*

For the rest of this paper let $\mathbb{K}$ be an algebraic number field, κ an arbitrary positive real, $\gamma \geqslant 1$ an integer and Γ a (not necessarily torsion-free) subgroup of $\mathbb{K}^*$ of rank γ.

2·1. *Averaging over all ideals*

For any positive integer n, we denote by $P^+(n)$ the largest prime divisor of n, or 1 if $n = 1$, and we set

$$\mathcal{P}_{\delta,\mathbb{K}}(y) = \left\{\mathfrak{p} : \mathcal{N}\mathfrak{p} \leqslant y,\ P^+(\mathcal{N}\mathfrak{p} - 1) < y^{\delta}\right\}$$

for any δ, $y > 0$. Then we obtain the following theorem.

THEOREM 1. *Let $\mathbb{K}$ be a number field. Assume that $\delta > 0$ is a positive constant such that there exist constants $K = K(\delta)$ and $y_0(\delta)$ for which*

$$\sharp\, \mathcal{P}_{\delta,\mathbb{K}}(y) \gg \frac{y}{(\log y)^K} \tag{2·1}$$

holds for all $y > y_0(\delta)$ with an implied constant possibly depending on $\mathbb{K}$. For any $\kappa > 0$ and any subgroup Γ of $\mathbb{K}^*$ of rank $\gamma \geqslant 1$ we then have

$$\sum_{\substack{\mathcal{N}\,\mathfrak{a}\leqslant x \\ \overline{\Gamma}\subset(\mathcal{O}_{\mathbb{K}}\,/\,\mathfrak{a})^*}} \mathrm{ind}_\Gamma(\mathfrak{a})^\kappa \geqslant x^{1+\kappa-\delta+o(1)},$$

where the implied constant depends on γ, κ and $\mathbb{K}$.

The accuracy of this lower bound depends on the quality of the smoothness condition (2·1). In case $\mathbb{K} = \mathbb{Q}$ one knows that (2·1) is satisfied for $\delta = 0.2961\ldots$ (cf. [**1**]). It is conjectured to hold for all $\delta > 0$ with any $K > 1$. We believe that this is also true for the case $\mathbb{K} \neq \mathbb{Q}$ and expect an asymptotic law like $\sum \mathrm{ind}_\Gamma(\mathfrak{a})^\kappa = x^{1+\kappa+o(1)}$ to hold. Rohrlich [**25**] has proved that (2·1) holds with $K = 1$ and some δ sufficiently close to 1 and depending on $\mathbb{K}$, thereby improving the lower bound in (1·2) for any fixed number field. We establish, partly on GRH, admissible values for δ which are in fact smaller than $1/2$.

THEOREM 2. *Let $\mathbb{K}^{(n)}$ be the normal closure of $\mathbb{K}\,/\,\mathbb{Q}$ in some algebraic closure of $\mathbb{K}$ and, for $l \in \mathbb{N}$, let ζ_l denote a primitive l-th root of unity. Then condition* (2·1) *is satisfied for $K = 2$ and every $\delta > \delta_0$, where δ_0 depends on $\mathbb{K}$ and may be chosen as follows*:

(i) *if $\mathbb{K}^{(n)}$ is abelian, then $\delta_0 := \frac{1}{2\sqrt{e}} = 0.303265\ldots$;*

(ii) *if GRH holds for the fields $\mathbb{K}^{(n)}(\zeta_l)$, $l \in \mathbb{N}$, then $\delta_0 := \frac{1}{2}\exp\left\{-\frac{1}{[\mathbb{K}^{(n)}:\mathbb{Q}]+1}\right\}$;*

(iii) *if* $\mathrm{Gal}(\mathbb{K}^{(n)}\,/\,\mathbb{Q})$ *has an abelian subgroup of index $\leqslant 4$, then $\delta_0 := \frac{1}{2} - \eta$ with some $\eta > 0$ depending on $\mathbb{K}$.*

The value of δ_0 in (ii) *can be slightly improved. For details and the exact value of η in* (iii) *we refer to Section* 4·2·2.

Theorem 1 is very surprising. On the one hand, as we shall see below, the index averaged over prime ideals is typically small. In view of Artin's conjecture on primitive roots and Wagstaff's heuristic this is not an unexpected phenomenon, as already mentioned above. On the other hand, results of Kurlberg [**12**] and Kurlberg and Pomerance [**13**] suggest that even within the set of all ideals the index is small with probability 1. Nevertheless it turns out that the number of (highly composite) ideals for which the index is exceptionally big is larger than expected.

2·2. *Averaging over prime ideals*

Let $\mathbb{L}\,/\,\mathbb{K}$ be a finite normal extension. For a non-empty conjugacy class C in its Galois group $\mathrm{Gal}(\mathbb{L}\,/\,\mathbb{K})$ we denote by $\mathcal{P}_C(\mathbb{L}\,/\,\mathbb{K})$ the set of all prime ideals $\mathfrak{p}$ of $\mathbb{K}$ which are unramified in $\mathbb{L}$ and satisfy $\left[\frac{\mathbb{L}|\mathbb{K}}{\mathfrak{p}}\right] = C$. Here $\left[\frac{\mathbb{L}|\mathbb{K}}{\mathfrak{p}}\right]$ is the Frobenius symbol of $\mathfrak{p}$. For convenience $\mathcal{P}_C(x, \mathbb{L}\,/\,\mathbb{K})$ will consist of all $\mathfrak{p} \in \mathcal{P}_C(\mathbb{L}\,/\,\mathbb{K})$ with norm $\leqslant x$, and $\pi_C(x, \mathbb{L}\,/\,\mathbb{K})$ will denote the corresponding counting function.

We are interested not only in lower bounds, but in the asymptotic behaviour of κ-th moments of $\mathrm{ind}_\Gamma(\mathfrak{p})$ taken over prime ideals $\mathfrak{p} \in \mathcal{P}_C(\mathbb{L}/\mathbb{K})$ which satisfy $\overline{\Gamma} \subset (\mathcal{O}_{\mathbb{K}}\,/\,\mathfrak{p})^*$. As explained in the introduction, it is hopeless to attack this task by common methods. We therefore sum the quantity

$$\mathcal{I}_\gamma^\kappa(\mathfrak{p}) := \sum_{a_1,\ldots,a_\gamma \in (\mathcal{O}_{\mathbb{K}}\,/\,\mathfrak{p})^*} \frac{\mathrm{ind}_{\langle a_1,\ldots,a_\gamma\rangle}(\mathfrak{p})^\kappa}{(\mathcal{N}\,\mathfrak{p}-1)^\gamma},$$

the κ-th moment of $\mathrm{ind}_{\langle a_1,\ldots,a_\gamma\rangle}(\mathfrak{p})$ averaged over all $(a_1, \ldots, a_\gamma) \in (\mathcal{O}_{\mathbb{K}}\,/\,\mathfrak{p})^{*\gamma}$. One may hope that the behaviour of the reduction of Γ modulo $\mathfrak{p}$ (whenever $\overline{\Gamma} \subset (\mathcal{O}_{\mathbb{K}} / \mathfrak{p})^*$) resembles that of a generic group, so that $\mathcal{I}_\gamma^\kappa(\mathfrak{p})$ yields a reasonable approximation of $\operatorname{ind}_\Gamma(\mathfrak{p})^\kappa$.

As a consequence of the additional averaging process, precise asymptotic estimates for the average order of $\mathcal{I}_\gamma^\kappa(\mathfrak{p})$ over prime ideals in $\mathcal{P}_C(\mathbb{L}/\mathbb{K})$ become available. We formulate these in the subsequent theorem. The results are unconditional and depend on whether $\gamma = \kappa$, $\gamma > \kappa$ or $\gamma < \kappa$. The latter two cases turn out to be easier and admit asymptotic formulae while in the first case one may at least determine the corresponding growth rate.

THEOREM 3. *Let $\mathbb{K}$, $\mathbb{L}$, C, κ and γ be as above. For a positive integer n we let*

$$c_C(n) = \begin{cases} |C|, & \textit{if } \{\sigma \in C : \sigma|_{\mathbb{L}\cap\mathbb{K}(\zeta_n)} = \mathrm{id}\} \neq \varnothing, \\ 0, & \textit{otherwise.} \end{cases}$$

Let furthermore $\varphi_t(n)$ be the multiplicative function defined by $\varphi_t(p^e) = p^e(1 - 1/p^t)$ for any prime power p^e, $e \geqslant 1$, and any real $t > 0$.

(i) *if $\gamma > \kappa$, then*

$$\sum_{\mathfrak{p}\in\mathcal{P}_C(x,\mathbb{L}/\mathbb{K})} \mathcal{I}_\gamma^\kappa(\mathfrak{p}) = \mathrm{li}(x) \cdot \sum_{n\geqslant 1} \frac{c_C(n)\varphi_\kappa(n)}{n^{\gamma-\kappa+1}[\mathbb{L}(\zeta_n) : \mathbb{K}]} + O\left(\frac{\mathrm{li}(x)}{(\log\log x)^{\frac{\gamma(\gamma-\kappa)}{2\gamma-\kappa}-\varepsilon}}\right),$$

where the implied constant depends on $\mathbb{L}$, γ, κ and ε, and the sum over n is convergent and positive;

(ii) *if $\gamma = \kappa$, then*

$$x \ll_{\mathbb{L}} \sum_{\mathfrak{p}\in\mathcal{P}_C(x,\mathbb{L}/\mathbb{K})} \mathcal{I}_\gamma^\gamma(\mathfrak{p}) \ll_{\mathbb{K}} x;$$

(iii) *if $\gamma < \kappa$, then*

$$\sum_{\mathfrak{p}\in\mathcal{P}_C(x,\mathbb{L}/\mathbb{K})} \mathcal{I}_\gamma^\kappa(\mathfrak{p}) = \mathrm{li}(x^{\kappa-\gamma+1}) \cdot \sum_{n\geqslant 1} \frac{c_C(n)\varphi_\gamma(n)}{n^{\kappa-\gamma+1}[\mathbb{L}(\zeta_n) : \mathbb{K}]} + O\left(\frac{\mathrm{li}(x^{\kappa-\gamma+1})}{(\log\log x)^{\frac{\kappa(\kappa-\gamma)}{2\kappa-\gamma}-\varepsilon}}\right),$$

where the implied constant depends on $\mathbb{L}$, γ, κ and ε, and the sum over n is convergent and positive.

As Theorem 4 will show, the asymptotic constant and the error terms in Theorem 3 (i) and (iii) can be simplified and improved, respectively, and Theorem 3 (ii) can be replaced by an asymptotic formula under GRH, if one additionally assumes that $\mathbb{L}$ and $\mathbb{K}$ are both normal over $\mathbb{Q}$. We conjecture that such an asymptotic formula holds in general.

THEOREM 4. *With the above notations assume that $\mathbb{L}$ and $\mathbb{K}$ are normal over $\mathbb{Q}$, and let m be some positive integer such that $\mathbb{L}^{ab}$, the abelian part of $\mathbb{L}$, is contained in $\mathbb{Q}(\zeta_m)$. Set*

$$A_\gamma^\kappa := A_\gamma^\kappa(\mathbb{L}/\mathbb{K}, C) := \frac{|C|}{[\mathbb{L} : \mathbb{K}]} \sum_{\substack{d|m \\ c_C(d)\neq 0}} \frac{[\mathbb{L}\cap\mathbb{Q}(\zeta_d) : \mathbb{Q}]\varphi_{\gamma-\kappa+1}\left(\frac{m}{d}\right) a_\gamma^\kappa(m,d)}{md^{\gamma-\kappa}},$$

with certain positive real numbers $a_\gamma^\kappa(m,d)$ given by Euler products which only depend on κ, γ, m and d and will be defined in Lemma 13. Then A_γ^κ is positive and we have:

(i) *if $\gamma > \kappa$, then*

$$\sum_{\mathfrak{p}\in\mathcal{P}_C(x,\mathbb{L}/\mathbb{K})} \mathcal{I}_\gamma^\kappa(\mathfrak{p}) = \zeta(\gamma-\kappa+1)A_\gamma^\kappa \,\mathrm{li}(x) + O\left(\frac{\mathrm{li}(x)}{(\log x)^{\frac{\gamma(\gamma-\kappa)}{6\gamma-3\kappa}-\varepsilon}}\right),$$

where $\zeta(s)$ denotes the Riemann zeta function and the implied constant depends on $\mathbb{L}$, γ, κ and ε;

(ii) *if $\gamma = \kappa$ and one assumes the GRH for the fields $\mathbb{L}(\zeta_n)$, $n \geqslant 1$, then*

$$\sum_{\mathfrak{p} \in \mathcal{P}_C(x, \mathbb{L}/\mathbb{K})} \mathcal{I}_\gamma^\gamma(\mathfrak{p}) = A_\gamma^\gamma x + O_{\mathbb{L}}\left(\frac{x \log\log x}{\log x}\right);$$

(iii) *if $\gamma < \kappa$, then*

$$\sum_{\mathfrak{p} \in \mathcal{P}_C(x, \mathbb{L}/\mathbb{K})} \mathcal{I}_\gamma^\kappa(\mathfrak{p}) = \zeta(\kappa - \gamma + 1) A_\kappa^\gamma \operatorname{li}(x^{\kappa - \gamma + 1}) + O\left(\frac{\operatorname{li}(x^{\kappa-\gamma+1})}{(\log x)^{\frac{\kappa(\kappa-\gamma)}{6\kappa - 3\gamma} - \varepsilon}}\right),$$

where the implied constant depends on $\mathbb{L}$, γ, κ and ε.

Remark 5. Although not obvious from its definition the constant A_γ^κ in Theorem 4 does not depend on the choice of m as will become clear in Section 3·3. Moreover, if $\kappa = 1$ then $a_\gamma^1(m, d) = 1$ holds for any γ and all $d \mid m$ (cf. Lemma 13) which simplifies A_γ^κ substantially.

Theorem 4 supports (1·3) and Wagstaff's heuristic in particular. Theorem 4 (ii) remains true unconditionally if Proposition 11, a generalisation of the classical Bombieri–Vinogradov Theorem, may be applied. This is the case, if $\mathbb{L} \cap \mathbb{Q}(\zeta_n) = \mathbb{Q}$ holds for all positive integers n, and the largest abelian subgroup H of $\mathrm{Gal}(\mathbb{L}/\mathbb{Q})$ for which $H \cap C \neq \varnothing$ has index $\leqslant 4$ inside $\mathrm{Gal}(\mathbb{L}/\mathbb{Q})$ (see Section 3·3 for more details). Hence, Theorem 4 (ii) generalises a recent result of Felix [**6**] who independently proved the statement for $\gamma = 1$ and $\mathbb{L} = \mathbb{Q}$.

At last, Theorem 3 (i) and (iii) hold with the better error terms of Theorem 4 if there exists a field tower $\mathbb{Q} = \mathbb{M}_0 \subset \mathbb{M}_1 \subset \cdots \subset \mathbb{M}_s = \mathbb{K}$ in which each field is normal over the preceding one. This is a consequence of stronger upper bounds for possible Siegel zeroes of Dedekind zeta functions (cf. Proposition 9). Further explanations will be provided at the end of Section 3·1.

2·3. *Structure and methods of this paper*

In Section 3 we proceed with the proofs of Theorems 3 and 4. The basic idea to estimate the average of $\mathcal{I}_\gamma^\kappa$ over the designated set of prime ideals of $\mathbb{K}$ is to interchange the summation order and then estimate the sizes of occurring sets of prime ideals by the Brun–Titchmarsh inequality [**28**, p. 73] and effective versions of the Čebotarev Density Theorem. In case $\gamma \neq \kappa$ it suffices to apply an unconditional version of the latter (cf. Proposition 8), whereas in case $\gamma = \kappa$ one needs to resort to a stronger version under GRH (cf. Proposition 12) to tackle the arising difficulties. These difficulties may in certain cases be overcome by the Bombieri–Vinogradov Theorem [**7**, p. 170] or an appropriate number field analogue thereof (cf. Proposition 11). All occurring implied constants which depend on $\mathbb{L}$ may also depend on $\mathbb{K}$ and C.

Theorems 1 and 2 are addressed in Section 4. The key ingredient underlying Theorem 1 is the estimate $\operatorname{ind}_\Gamma(\mathfrak{a}) \gg \varphi(\mathfrak{a})/\lambda(\mathfrak{a})^\gamma$, where $\varphi(\mathfrak{a})$ and $\lambda(\mathfrak{a})$ denote order and exponent of $(\mathcal{O}_{\mathbb{K}}/\mathfrak{a})^*$, respectively. We establish lower bounds for moments of $\operatorname{ind}_\Gamma(\mathfrak{a})$ by constructing sufficiently many highly composite ideals $\mathfrak{a}$ for which this ratio becomes exceptionally large, thereby generalising a result of Luca and Sankaranarayanan [**18**]. Theorem 2 is proved by adapting classical ideas of Balog [**2**] and Friedlander [**8**] to number fields. The quality of this adaption, and hence the accuracy of the admissible values in Theorem 2, again depends on the effective versions of the Čebotarev Density Theorem and number field analogues of the Bombieri–Vinogradov Theorem, respectively, one may apply.

To conclude with we note that the average behaviour of the order, in some sense the counterpart of the index, has been studied intensively and often appears to be the easier problem. In [**13**] Kurlberg and Pomerance have established sharp upper and lower bounds for the average order of $\operatorname{ord}_a(n)$ over all integers n on the one hand, and on the other hand they proved an asymptotic formula for the average order of $\operatorname{ord}_a(p)$ over primes p subject to the GRH for certain number fields. Using the same methods, these results seem to admit similar statements in the more general setting of a number field $\mathbb{K}$ and a finitely generated subgroup Γ of $\mathbb{K}^*$.

3. *Averaging over prime ideals*

To start with, we note that

$$\mathcal{I}_\gamma^\kappa(\mathfrak{p}) = \frac{1}{(\mathcal{N}\mathfrak{p}-1)^\gamma} \sum_{d \mid \mathcal{N}\mathfrak{p}-1} d^\kappa \sum_{f \mid \frac{\mathcal{N}\mathfrak{p}-1}{d}} \mu(f) h_{\gamma,\mathfrak{p}}\left(\frac{\mathcal{N}\mathfrak{p}-1}{df}\right),$$

where $h_{\gamma,\mathfrak{p}}(n)$ denotes the number of γ-tupels $(a_1, \ldots, a_\gamma) \in (\mathcal{O}_\mathbb{K}/\mathfrak{p})^{*\gamma}$ for which the order of $\langle a_1, \ldots, a_\gamma \rangle$ divides n. Since $(\mathcal{O}_\mathbb{K}/\mathfrak{p})^*$ is cyclic one clearly has $h_{\gamma,\mathfrak{p}}(n) = n^\gamma$ for any divisor n of $\mathcal{N}\mathfrak{p}-1$. Hence

$$\mathcal{I}_\gamma^\kappa(\mathfrak{p}) = \sum_{d \mid \mathcal{N}\mathfrak{p}-1} \frac{1}{d^{\gamma-\kappa}} \sum_{f \mid \frac{\mathcal{N}\mathfrak{p}-1}{d}} \frac{\mu(f)}{f^\gamma}. \tag{3·1}$$

Summing over $\mathfrak{p} \in \mathcal{P}_C(\mathbb{L}/\mathbb{K})$ we thus obtain

$$\sum_{\mathfrak{p} \in \mathcal{P}_C(x,\mathbb{L}/\mathbb{K})} \mathcal{I}_\gamma^\kappa(\mathfrak{p}) = \sum_{\mathfrak{p} \in \mathcal{P}_C(x,\mathbb{L}/\mathbb{K})} \sum_{d \mid \mathcal{N}\mathfrak{p}-1} \frac{1}{d^{\gamma-\kappa}} \sum_{f \mid (\mathcal{N}\mathfrak{p}-1)/d} \frac{\mu(f)}{f^\gamma}. \tag{3·2}$$

This formula turns out to be a vital tool in case $\gamma \geqslant \kappa$. In case $\kappa > \gamma$, however, the term $1/d^{\gamma-\kappa}$ causes troubles, and it is more convenient to consider

$$\sum_{\mathfrak{p} \in \mathcal{P}_C(x,\mathbb{L}/\mathbb{K})} \frac{\mathcal{I}_\gamma^\kappa(\mathfrak{p})}{(\mathcal{N}\mathfrak{p}-1)^{\kappa-\gamma}} = \sum_{\mathfrak{p} \in \mathcal{P}_C(x,\mathbb{L}/\mathbb{K})} \sum_{d \mid \mathcal{N}\mathfrak{p}-1} \frac{1}{d^{\kappa-\gamma}} \sum_{f \mid d} \frac{\mu(f)}{f^\gamma}, \tag{3·3}$$

which is easily derived if one exchanges the roles of d and $(\mathcal{N}\mathfrak{p}-1)/d$ in (3·1). We start with the proof of Theorem 3 and first consider parts (i) and (iii), as it turns out to be more convenient to treat the cases $\kappa = \gamma$ and $\kappa \neq \gamma$ separately.

3·1. *Proof of Theorem* 3 (i) *and* (iii)

Rearranging the right-hand sides of (3·2) and (3·3) yields

$$\sum_{\mathfrak{p} \in \mathcal{P}_C(x,\mathbb{L}/\mathbb{K})} \mathcal{I}_\gamma^\kappa(\mathfrak{p}) = \sum_{f \leqslant x} \frac{\mu(f)}{f^\gamma} \sum_{d \leqslant x} \frac{1}{d^{\gamma-\kappa}} \sum_{\substack{\mathfrak{p} \in \mathcal{P}_C(x,\mathbb{L}/\mathbb{K}) \\ \mathcal{N}\mathfrak{p} \equiv 1\ (df)}} 1, \tag{3·4}$$

in case $\gamma > \kappa$, and

$$\sum_{\mathfrak{p} \in \mathcal{P}_C(x,\mathbb{L}/\mathbb{K})} \frac{\mathcal{I}_\gamma^\kappa(\mathfrak{p})}{(\mathcal{N}\mathfrak{p}-1)^{\kappa-\gamma}} = \sum_{f \leqslant x} \frac{\mu(f)}{f^\kappa} \sum_{d \leqslant x} \frac{1}{d^{\kappa-\gamma}} \sum_{\substack{\mathfrak{p} \in \mathcal{P}_C(x,\mathbb{L}/\mathbb{K}) \\ \mathcal{N}\mathfrak{p} \equiv 1\ (df)}} 1, \tag{3·5}$$

for $\gamma < \kappa$. Observing (3·4) and (3·5), we notice that the respective right-hand sides are almost identical, only κ and γ have swapped their roles. It therefore suffices to study the case $\gamma > \kappa$ by the right-hand side of (3·4), and transfer the results to the case $\kappa > \gamma$ later on.

Henceforth we thus assume $\gamma > \kappa$ until further notice. To get rid of the terms for large d and f we prove the following lemma.

LEMMA 6. *For any positive parameters* $1 < y, z \leqslant x^\alpha$ *with* $0 < \alpha < 1/2$ *we have*

$$\sum_{f\leqslant x}\frac{\mu(f)}{f^\gamma}\sum_{d\leqslant x}\frac{1}{d^{\gamma-\kappa}}\sum_{\substack{\mathfrak{p}\in\mathcal{P}_C(x,\mathbb{L}/\mathbb{K})\\ \mathcal{N}\mathfrak{p}\equiv 1\ (df)}}1=\sum_{f\leqslant y}\frac{\mu(f)}{f^\gamma}\sum_{d\leqslant z}\frac{1}{d^{\gamma-\kappa}}\sum_{\substack{\mathfrak{p}\in\mathcal{P}_C(x,\mathbb{L}/\mathbb{K})\\ \mathcal{N}\mathfrak{p}\equiv 1\ (df)}}1$$
$$+O\left(x^{2/3}+\frac{x}{x^{\alpha(\gamma-\kappa)}}+\frac{\mathrm{li}(x)}{y^\gamma}+\frac{\mathrm{li}(x)}{z^{\gamma-\kappa}}\right),$$

where the implied constant depends on $\mathbb{K}$, γ *and* κ.

Proof. The sum over $\mathfrak{p}$ is trivially bounded from above by $[\mathbb{K}:\mathbb{Q}]x/(df)$. Recalling that $\gamma \geqslant 1$ and $\gamma > \kappa$ we thus obtain

$$\sum_{f>x^\alpha}\frac{\mu(f)}{f^\gamma}\sum_{d\leqslant x}\frac{1}{d^{\gamma-\kappa}}\sum_{\substack{\mathfrak{p}\in\mathcal{P}_C(x,\mathbb{L}/\mathbb{K})\\ \mathcal{N}\mathfrak{p}\equiv 1\ (df)}}1 \ll_{\mathbb{K}} x\sum_{f>x^\alpha}\frac{1}{f^{\gamma+1}}\sum_{d\leqslant x}\frac{1}{d^{\gamma-\kappa+1}} \ll_{\gamma,\kappa} x^{1-\gamma\alpha} \ll \frac{x}{x^{\alpha(\gamma-\kappa)}}$$

and

$$\sum_{f\leqslant x}\frac{\mu(f)}{f^\gamma}\sum_{d>x^\alpha}\frac{1}{d^{\gamma-\kappa}}\sum_{\substack{\mathfrak{p}\in\mathcal{P}_C(x,\mathbb{L}/\mathbb{K})\\ \mathcal{N}\mathfrak{p}\equiv 1\ (df)}}1 \ll_{\mathbb{K}} x\sum_{f\leqslant x}\frac{1}{f^{\gamma+1}}\sum_{d>x^\alpha}\frac{1}{d^{\gamma-\kappa+1}} \ll_{\gamma,\kappa} \frac{x}{x^{\alpha(\gamma-\kappa)}}.$$

It remains to estimate the terms with $d, f \leqslant x^\alpha$ and $f > y$ or $d > z$. The contribution of non-linear prime ideals of $\mathbb{K}$ is bounded by $O_{\mathbb{K}}(x^{2/3})$ as one can easily see from (3·2) and standard estimates for divisor functions. Writing $\pi(x; a, q)$ for the number of primes up to x in the arithmetic progression a modulo q the Brun-Titchmarsh inequality yields

$$\sum_{y<f\leqslant x^\alpha}\frac{\mu(f)}{f^\gamma}\sum_{d\leqslant x^\alpha}\frac{1}{d^{\gamma-\kappa}}\sum_{\substack{\mathfrak{p}\in\mathcal{P}_C(x,\mathbb{L}/\mathbb{K})\\ \mathcal{N}\mathfrak{p}\equiv 1\ (df)}}1 \ll_{\mathbb{K}} \sum_{y<f\leqslant x^\alpha}\frac{\mu(f)}{f^\gamma}\sum_{d\leqslant x^\alpha}\frac{\pi(x;1,df)}{d^{\gamma-\kappa}}+x^{2/3}$$
$$\ll_{\gamma,\kappa}\frac{\mathrm{li}(x)}{y^\gamma}+x^{2/3}.$$

Here we used the trivial estimates $\varphi(mn) \geqslant \varphi(m)\varphi(n)$ for Euler's totient function and $\sum_{n\geqslant x}1/(n^r\varphi(n)) = O_r(x^{-r})$ valid for any $r > 0$. In the same way one deduces

$$\sum_{f\leqslant x^\alpha}\frac{\mu(f)}{f^\gamma}\sum_{z<d\leqslant x^\alpha}\frac{1}{d^{\gamma-\kappa}}\sum_{\substack{\mathfrak{p}\in\mathcal{P}_C(x,\mathbb{L}/\mathbb{K})\\ \mathcal{N}\mathfrak{p}\equiv 1\ (df)}}1 \ll_{\mathbb{K},\gamma,\kappa}\frac{\mathrm{li}(x)}{z^{\gamma-\kappa}}+x^{2/3},$$

and the assertion follows.

Now choose parameters $1 \leqslant y, z \leqslant x^{1/3}$ which we specify later. Lemma 6 then yields

$$\sum_{\mathfrak{p}\in\mathcal{P}_C(x,\mathbb{L}/\mathbb{K})}\mathcal{I}_\gamma^\kappa(\mathfrak{p})=\sum_{f\leqslant y}\frac{\mu(f)}{f^\gamma}\sum_{d\leqslant z}\frac{1}{d^{\gamma-\kappa}}\sum_{\substack{\mathfrak{p}\in\mathcal{P}_C(x,\mathbb{L}/\mathbb{K})\\ \mathcal{N}\mathfrak{p}\equiv 1\ (df)}}1+O\left(x^{2/3}+\frac{x}{x^{(\gamma-\kappa)/3}}+\frac{\mathrm{li}(x)}{y^\gamma}+\frac{\mathrm{li}(x)}{z^{\gamma-\kappa}}\right) \tag{3·6}$$

with an implied constant depending on $\mathbb{K}$, γ and κ. For any positive integer n we set $\mathbb{K}_n := \mathbb{K}(\zeta_n)$ and $\mathbb{L}_n := \mathbb{L}(\zeta_n)$, both being finite normal extensions of $\mathbb{K}$. By a standard argument from algebraic number theory, the condition $\mathcal{N}\mathfrak{p} \equiv 1\ (df)$ is equivalent to the complete splitting of $\mathfrak{p}$ in the normal extension $\mathbb{K}_{df} / \mathbb{K}$ (cf. [**23**, p. 50]). Thus the prime ideals $\mathfrak{p} \in \mathcal{P}_C(\mathbb{L}/\mathbb{K})$ which satisfy $\mathcal{N}\mathfrak{p} \equiv 1\ (df)$ are exactly those which are unramified in $\mathbb{L}_{df}$ and satisfy $\left[\frac{\mathbb{L}_{df}|\mathbb{K}}{\mathfrak{p}}\right] \subset C(df)$, where

$$C(n) := \{\sigma \in \mathrm{Gal}(\mathbb{L}_n / \mathbb{K}) : \sigma|_{\mathbb{L}} \in C, \sigma|_{\mathbb{K}_n} = \mathrm{id}\}$$

for any positive integer n.

LEMMA 7. *$C(n)$ is either empty or a conjugacy class in* $\mathrm{Gal}(\mathbb{L}_n / \mathbb{K})$*, and we have*

$$|C(n)| = c_C(n),$$

where $c_C(n)$ is as defined in the statement of Theorem 3.

Proof. Clearly $|C(n)| \neq 0$ implies $c_C(n) \neq 0$. If $c_C(n) \neq 0$, let σ lie in the intersection of C and $\mathrm{Gal}(\mathbb{L} / \mathbb{L} \cap \mathbb{K}_n)$. Since $\mathbb{L}_n / \mathbb{L} \cap \mathbb{K}_n$ is the direct product of the extensions $\mathbb{L} / \mathbb{L} \cap \mathbb{K}_n$ and $\mathbb{K}_n / \mathbb{L} \cap \mathbb{K}_n$, there exists a lift $\tilde{\sigma}$ of σ in $\mathrm{Gal}(\mathbb{L}_n / \mathbb{L} \cap \mathbb{K}_n)$ satisfying $\tilde{\sigma}|_{\mathbb{K}_n} = \mathrm{id}$ (cf. [**10**, p. 131]). Hence $\tilde{\sigma} \in C(n)$ showing that $C(n)$ is empty if and only if $c_C(n) = 0$.

Assume that $C(n)$ is not empty and let $\sigma \in C(n)$. Note that $C(n)$ is clearly closed under conjugation because $\mathbb{L}$ and $\mathbb{K}_n$ are normal over $\mathbb{K}$. Since $\tau\sigma\tau^{-1}|_{\mathbb{L}}$ runs through C as τ runs through $\mathrm{Gal}(\mathbb{L}_n / \mathbb{K})$, $C(n)$ contains a conjugacy class of $\mathrm{Gal}(\mathbb{L}_n / \mathbb{K})$ with at least $|C|$ elements. On the other hand the map $C(n) \to C$, $\sigma \mapsto \sigma|_{\mathbb{L}}$ is injective because $\mathbb{L}_n = \mathbb{L}\mathbb{K}_n$. This yields $|C(n)| \leqslant |C|$ and proves that $C(n)$ must be a conjugacy class.

Thus the sum over $\mathfrak{p}$ on the right-hand side of (3·6) may be written as $\pi_{C(df)}(x, \mathbb{L}_{df} / \mathbb{K})$. Such quantities are estimated using effective versions of the Čebotarev Density Theorem as provided by the following result due to Lagarias and Odlyzko [**14**].

PROPOSITION 8 (Lagarias–Odlyzko). *Let $\mathbb{L}' / \mathbb{K}'$ be an arbitrary normal extension of number fields and $C' \subset$* $\mathrm{Gal}(\mathbb{L}' / \mathbb{K}')$ *a conjugacy class or empty. Then there exist absolute constants $c_1, c_2 > 0$ such that, if* $\log x \geqslant 10[\mathbb{L}' : \mathbb{Q}](\log \Delta_{\mathbb{L}'})^2$, *then*

$$\left|\pi_{C'}(x, \mathbb{L}' / \mathbb{K}') - \frac{|C'|}{[\mathbb{L}' : \mathbb{K}']}\,\mathrm{li}(x)\right| \leqslant \frac{|C'|}{[\mathbb{L}' : \mathbb{K}']}\,\mathrm{li}(x^{\beta_0(\mathbb{L}')}) + c_1 x e^{-c_2\left(\frac{\log x}{[\mathbb{L}':\mathbb{Q}]}\right)^{1/2}},$$

where $\Delta_{\mathbb{L}'}$ denotes the discriminant of $\mathbb{L}'$, and $\beta_0(\mathbb{L}')$ constitutes the only possible zero of the Dedekind zeta function $\zeta_{\mathbb{L}'}(s)$ of $\mathbb{L}'$, $s = \sigma + it$, in the strip

$$1 - (4\log \Delta_{\mathbb{L}'})^{-1} \leqslant \sigma \leqslant 1, \quad |t| \leqslant (4\log \Delta_{\mathbb{L}'})^{-1},$$

which must therefore be simple and real.

Now choose y and z according to the condition $\log x \gg_{\mathbb{L}} (yz)^3 \log^2(yz)$. Invoking Proposition 8 and Lemma 7 we infer from (3·6)

$$\begin{aligned}\sum_{\mathfrak{p}\in\mathcal{P}_C(x,\mathbb{L}/\mathbb{K})} \mathcal{I}_\gamma^\kappa(\mathfrak{p}) &= \mathrm{li}(x)\sum_{f\leqslant y}\frac{\mu(f)}{f^\gamma}\sum_{d\leqslant z}\frac{c_C(df)}{d^{\gamma-\kappa}[\mathbb{L}_{df}:\mathbb{K}]} + O\left(\frac{\mathrm{li}(x)}{y^\gamma}+\frac{\mathrm{li}(x)}{z^{\gamma-\kappa}}\right)+E\\ &= \mathrm{li}(x)\sum_{f\geqslant 1}\frac{\mu(f)}{f^\gamma}\sum_{d\geqslant 1}\frac{c_C(df)}{d^{\gamma-\kappa}[\mathbb{L}_{df}:\mathbb{K}]} + O\left(\frac{\mathrm{li}(x)}{y^\gamma}+\frac{\mathrm{li}(x)}{z^{\gamma-\kappa}}\right)+E\\ &= \mathrm{li}(x)\sum_{n\geqslant 1}\frac{c_C(n)\varphi_\kappa(n)}{n^{\gamma-\kappa+1}[\mathbb{L}_n:\mathbb{K}]} + O\left(\frac{\mathrm{li}(x)}{y^\gamma}+\frac{\mathrm{li}(x)}{z^{\gamma-\kappa}}\right)+E \qquad (3{\cdot}7)\end{aligned}$$

with an implied constant depending on γ, κ and $\mathbb{L}$, since

$$[\mathbb{L}_n:\mathbb{K}] \geqslant [\mathbb{L}_n:\mathbb{L}] = \frac{[\mathbb{L}_n:\mathbb{Q}(\zeta_n)][\mathbb{Q}(\zeta_n):\mathbb{Q}]}{[\mathbb{L}:\mathbb{Q}]} \gg_{\mathbb{L}} \varphi(n). \qquad (3{\cdot}8)$$

The sum in (3·7) clearly converges absolutely because of $0 \leqslant c_C(n) \leqslant |C|$, $\gamma > \kappa$ and (3·8), and it is positive because the first summand is so and all others are $\geqslant 0$.

To estimate the error term E coming from Proposition 8 we need upper bounds for $\beta_0(\mathbb{L}_{df})$ and $\Delta_{\mathbb{L}_{df}}$. Sufficient results are given by the next two statements, the first of which is due to Stark [**27**, p. 148].

PROPOSITION 9 (Stark). *Let $\mathbb{L}'$ be a number field and set $m_{\mathbb{L}'} = 4$ if $\mathbb{L}'/\mathbb{Q}$ is normal, $m_{\mathbb{L}'} = 16$ if there exists a field tower $\mathbb{Q} = \mathbb{M}_0 \subset \mathbb{M}_1 \subset \cdots \subset \mathbb{M}_s = \mathbb{L}'$ with each field normal over the preceding one, and $m_{\mathbb{L}'} = 4[\mathbb{L}':\mathbb{Q}]!$ otherwise. Then there exists an absolute positive constant c_3, such that*

$$\beta_0 < \max\left\{1-\frac{1}{m_{\mathbb{L}'}\log\Delta_{\mathbb{L}'}},\ 1-\frac{1}{c_3\Delta_{\mathbb{L}'}^{1/[\mathbb{L}':\mathbb{Q}]}}\right\}.$$

LEMMA 10. *Let $\mathbb{L}'$ be a number field, k a positive integer and* $\mathrm{rad}(k)$ *its largest squarefree divisor. Then there exist positive constants c_4, c_5 which only depend on $\mathbb{L}'$ such that*

$$\Delta_{\mathbb{L}'(\zeta_k)} \leqslant \Big(c_4\varphi(k)\,\mathrm{rad}(k)\Big)^{c_5\varphi(k)}.$$

Proof. Let $\mathcal{P}$ be the set of primes which ramify in $\mathbb{L}'(\zeta_k)^{(n)}$, the normal closure of $\mathbb{L}'(\zeta_k)/\mathbb{Q}$ in some algebraic closure, and observe that $\Delta_{\mathbb{L}'(\zeta_k)}$ divides $\Delta^{(n)}_{\mathbb{L}'(\zeta_k)}$ (cf. [**23**, p. 213]). By [**26**, proposition 6] we obtain

$$\Delta_{\mathbb{L}'(\zeta_k)} \leqslant \left([\mathbb{L}'(\zeta_k)^{(n)}:\mathbb{Q}]\prod_{p\in\mathcal{P}} p\right)^{[\mathbb{L}'(\zeta_k)^{(n)}:\mathbb{Q}]}. \qquad (3{\cdot}9)$$

Now observe that the degree of $\mathbb{L}'(\zeta_k)^{(n)}$ over $\mathbb{L}'(\zeta_k)$ only depends on $\mathbb{L}'$, and $\mathcal{P}$ consists of those primes which divide k or the discriminant of $\mathbb{K}$. The assertion then follows by standard estimates for degrees of cyclotomic field extensions.

For n large enough we therefore obtain

$$\beta_0(\mathbb{L}_n) \leqslant 1-\frac{1}{8[\mathbb{L}_n:\mathbb{Q}][\mathbb{L}_n:\mathbb{Q}]!\log n} \leqslant 1-\frac{1}{(n[\mathbb{L}:\mathbb{Q}])^{n[\mathbb{L}:\mathbb{Q}]}} \qquad (3{\cdot}10)$$

by Proposition 9, Lemma 10 and Stirling's formula. Hence, by Proposition 8, Lemma 10 and (3·10) there exists a positive constant c depending on $\mathbb{L}$ such that

$$E \ll_{\mathbb{L}} \sum_{f \leqslant y} \frac{1}{f^{\gamma}} \sum_{d \leqslant z} \frac{1}{d^{\gamma-\kappa}} \left[\frac{1}{\varphi(df)} \operatorname{li}(x^{\beta_0(\mathbb{L}_{df})}) + xe^{-c\left(\frac{\log x}{[\mathbb{L}_{df}:\mathbb{Q}]}\right)^{1/2}} \right] \tag{3·11}$$

$$\ll_{\mathbb{L}} \operatorname{li}(x) \exp\left\{ -\frac{\log x}{(yz[\mathbb{L} : \mathbb{Q}])^{yz[\mathbb{L}:\mathbb{Q}]}} \right\} + zxe^{-c'\left(\frac{\log x}{yz}\right)^{1/2}}. \tag{3·12}$$

Here $c' > 0$ is another appropriate constant depending on $\mathbb{L}$. In view of (3·7) and (3·12) we set

$$y = (\log\log x)^{\frac{\gamma-\kappa}{(2\gamma-\kappa)}-\varepsilon} \qquad \text{and} \qquad z = (\log\log x)^{\frac{\gamma}{(2\gamma-\kappa)}-\varepsilon},$$

which yields the asserted asymptotic formula

$$\sum_{\mathfrak{p} \in \mathcal{P}_C(x,\mathbb{L}/\mathbb{K})} \mathcal{I}_{\gamma}^{\kappa}(\mathfrak{p}) = \operatorname{li}(x) \sum_{n \geqslant 1} \frac{c_C(n)\varphi_{\kappa}(n)}{n^{\gamma-\kappa+1}[\mathbb{L}_n : \mathbb{K}]} + O\left(\frac{\operatorname{li}(x)}{(\log\log x)^{\frac{\gamma(\gamma-\kappa)}{2\gamma-\kappa}-\varepsilon}} \right). \tag{3·13}$$

The corresponding asymptotic formula in case $\kappa > \gamma$ may be deduced from (3·5) by the same methods as above followed by a simple partial summation argument, and the proof of Theorem 3 is complete.

While we are on the subject of error terms, let us for the ease of readability include at this point the corresponding estimations in the situation of Theorem 4 and briefly show how to improve the error term in (3·13) if we assume the existence of a field tower $\mathbb{Q} = \mathbb{M}_0 \subset \mathbb{M}_1 \subset \cdots \subset \mathbb{M}_s = \mathbb{K}$ in which each field is normal over the preceding one. In this case, such a tower exists for any $\mathbb{L}_n$, too, and Proposition 9 and Lemma 10 provide the stronger bound $\beta_0(\mathbb{L}_n) \leqslant 1 - (c_3 n^2)^{-1}$ instead of (3·10), if n is large enough. From (3·11) we thus derive

$$E \ll_{\mathbb{L}} \operatorname{li}(x) e^{-\frac{\log x}{c_3(yz)^2}} + zxe^{-c'\left(\frac{\log x}{yz}\right)^{1/2}}.$$

Collecting error terms and recalling the condition $\log x \gg_{\mathbb{L}} (yz)^3 \log^2(yz)$, an optimization of y and z provides the choice

$$y = (\log x)^{\frac{\gamma-\kappa}{(6\gamma-3\kappa)}-\varepsilon} \qquad \text{and} \qquad z = (\log x)^{\frac{\gamma}{(6\gamma-3\kappa)}-\varepsilon}$$

and yields

$$\sum_{\mathfrak{p} \in \mathcal{P}_C(x,\mathbb{L}/\mathbb{K})} \mathcal{I}_{\gamma}^{\kappa}(\mathfrak{p}) = \operatorname{li}(x) \sum_{n \geqslant 1} \frac{c_C(n)\varphi_{\kappa}(n)}{n^{\gamma-\kappa+1}[\mathbb{L}_n : \mathbb{K}]} + O\left(\frac{\operatorname{li}(x)}{(\log x)^{\frac{\gamma(\gamma-\kappa)}{6\gamma-3\kappa}-\varepsilon}} \right). \tag{3·14}$$

Just as above, it is easy to derive an analogous error term in case $\kappa > \gamma$. In this way we have confirmed the remark in the last paragraph of Section 2·2 and already proved half of Theorem 4, too.

3·2. *Proof of Theorem* 3 (ii)

From (3·1) we initially infer the estimate

$$\mathcal{I}_{\gamma}^{\kappa}(\mathfrak{p}) \leqslant \sum_{d \mid \mathcal{N}\mathfrak{p}-1} d^{\kappa-\gamma} \leqslant \max\{1, (\mathcal{N}\mathfrak{p}-1)^{\kappa-\gamma}\}\tau(\mathcal{N}\mathfrak{p}-1) \tag{3·15}$$

valid for arbitrary $\gamma \geqslant 1$ and $\kappa > 0$, where $\tau(n)$ is the number of divisors of n. Now assume $\gamma = \kappa$. The asserted upper bound follows by a famous result of Linnik (cf. [**16**]):

$$\sum_{\mathfrak{p}\in\mathcal{P}_C(x,\mathbb{L}/\mathbb{K})} \mathcal{I}_\gamma^\gamma(\mathfrak{p}) \ll_{\mathbb{K}} \sum_{\substack{\mathcal{N}\mathfrak{p}\leqslant x\\ \mathfrak{p}\text{ linear}}} \tau(\mathcal{N}\mathfrak{p}-1) + x^{2/3} \ll_{\mathbb{K}} \sum_{p\leqslant x} \tau(p-1) + x^{2/3} \ll x.$$

Invoking (3·2) we find

$$\sum_{\mathfrak{p}\in\mathcal{P}_C(x,\mathbb{L}/\mathbb{K})} \mathcal{I}_\gamma^\gamma(\mathfrak{p}) = \sum_{d\leqslant x} \frac{\varphi_\gamma(d)}{d} \sum_{\substack{\mathfrak{p}\in\mathcal{P}_C(x,\mathbb{L}/\mathbb{K})\\ d\mid\mathcal{N}\mathfrak{p}-1}} 1 \geqslant \sum_{d\leqslant x} \frac{\varphi(d)}{d} \sum_{\substack{\mathfrak{p}\in\mathcal{P}_C(x,\mathbb{L}/\mathbb{K})\\ d\mid\mathcal{N}\mathfrak{p}-1}} 1. \tag{3·16}$$

To estimate the sum over $\mathfrak{p}$ in (3·16) we quote the following generalisation of the classical Bombieri–Vinogradov Theorem which combines a result of Murty and Murty [**20**] and a recent generalisation thereof due to Murty and Petersen [**21**]. This result allows appropriate unconditional estimates for the error term in Proposition 8 on average over large moduli.

PROPOSITION 11 (Murty–Murty–Petersen). *Let $\mathbb{L}'\,/\,\mathbb{K}'$ be an arbitrary normal extension of number fields and $C' \subset \mathrm{Gal}(\mathbb{L}'\,/\,\mathbb{K}')$ a conjugacy class or empty. For integers a and $q > 0$ let $\pi_{C'}(x; a, q)$ denote the number of prime ideals $\mathfrak{p}$ of $\mathbb{K}'$ which are unramified in $\mathbb{L}'$ and satisfy $\mathcal{N}\mathfrak{p} \leqslant x$, $\mathcal{N}\mathfrak{p} \equiv a\ (q)$ and $\left[\frac{\mathbb{L}'|\mathbb{K}'}{\mathfrak{p}}\right] = C'$. Let H be the largest abelian subgroup of $\mathrm{Gal}(\mathbb{L}'\,/\,\mathbb{K}')$ such that $H \cap C' \neq \varnothing$ and denote by $\mathbb{M}'$ the fixed field of H. Finally, set $\eta = \max\{[\mathbb{M}' : \mathbb{Q}] - 2, 2\}$ and $Q = x^{\frac{1}{\eta}-\varepsilon}$. Then for any $A > 0$ we have*

$$\sum_{\substack{q\leqslant Q\\ \mathbb{L}'\cap\mathbb{Q}(\zeta_q)=\mathbb{Q}}} \max_{(a,q)=1} \max_{y\leqslant x} \left| \pi_{C'}(y; a, q) - \frac{|C'|}{\varphi(q)[\mathbb{L}' : \mathbb{K}']}\pi(y) \right| \ll_{\varepsilon,A} \frac{x}{\log^A x}.$$

If $\mathbb{K}' = \mathbb{Q}$ this result remains true with $Q = x^{\frac{1}{\eta}} \log^{-B} x$, where $B = B(A)$ is a positive constant depending on A.

To apply this result we need to restrict the range of the moduli d in (3·16) a little further. Any positive integer d for which $(d, \Delta_{\mathbb{L}}) = 1$ holds also satisfies $(\Delta_{\mathbb{Q}(\zeta_d)}, \Delta_{\mathbb{L}}) = 1$ (cf. [**30**, proposition 2·7]). Hence, $[\mathbb{L}_d : \mathbb{L}] = \varphi(d)$ and $\mathbb{L} \cap \mathbb{Q}(\zeta_d) = \mathbb{Q}$ hold whenever $(d, \Delta_{\mathbb{L}}) = 1$ (cf. [**9**, p. 98]). Since primes dividing $\Delta_{\mathbb{K}}$ must divide $\Delta_{\mathbb{L}}$ the same holds for $\mathbb{K}_d\,/\,\mathbb{K}$. Thus we deduce that $[\mathbb{L} \cap \mathbb{K}_d] = \mathbb{K}$ (cf. [**10**, p. 131]) and hence $|C(d)| = |C|$ by Lemma 7. For $0 < \alpha < 1/2$ sufficiently small we finally obtain

$$\sum_{\mathfrak{p}\in\mathcal{P}_C(x,\mathbb{L}/\mathbb{K})} \mathcal{I}_\gamma^\gamma(\mathfrak{p}) \geqslant \sum_{\substack{d\leqslant x^\alpha\\ (d,\Delta_{\mathbb{L}})=1}} \frac{\varphi(d)}{d} \sum_{\substack{\mathfrak{p}\in\mathcal{P}_C(x,\mathbb{L}/\mathbb{K})\\ d\mid\mathcal{N}\mathfrak{p}-1}} 1 \gg_{\mathbb{L}} \pi(x) \sum_{\substack{d\leqslant x^\alpha\\ (d,\Delta_{\mathbb{L}})=1}} \frac{1}{d} \gg_{\mathbb{L}} x,$$

by Proposition 11 and Möbius inversion.

3·3. *Proof of Theorem* 4

Let us now assume that $\mathbb{L}\,/\,\mathbb{Q}$ and $\mathbb{K}\,/\,\mathbb{Q}$ are both normal. The advantage here is the additional action of $\mathrm{Gal}(\mathbb{K}\,/\,\mathbb{Q})$ and $\mathrm{Gal}(\mathbb{L}\,/\,\mathbb{Q})$ on the prime ideals of $\mathbb{K}$ and $\mathbb{L}$, respectively. By the same arguments as in Section 3·1 we may without loss of generality assume $\gamma \geqslant \kappa$. To begin with we note that one may neglect non-linear prime ideals of $\mathbb{K}$, since there are only $O_{\mathbb{K}}(\sqrt{x})$ such prime ideals with norm $\leqslant x$, whence

$$\sum_{\mathfrak{p}\in\mathcal{P}_C(x,\mathbb{L}/\mathbb{K})} \mathcal{I}_\gamma^\kappa(\mathfrak{p}) = \sum_{\substack{\mathfrak{p}\in\mathcal{P}_C(x,\mathbb{L}/\mathbb{K})\\ \mathfrak{p} \text{ linear}}} \mathcal{I}_\gamma^\kappa(\mathfrak{p}) + O_{\mathbb{K}}(x^{2/3})$$

by (3·15) and a trivial estimate for the divisor function.

Now let $\sigma \in C$ and let $\mathscr{C}$ be the conjugacy class of σ in $\mathrm{Gal}(\mathbb{L}/\mathbb{Q})$. Clearly, we have $C \subset \mathscr{C} \subset \mathrm{Gal}(\mathbb{L}/\mathbb{K})$ because $\mathbb{K}/\mathbb{Q}$ is normal. If $\mathcal{Z}(\sigma)$ denotes the centraliser of σ in $\mathrm{Gal}(\mathbb{L}/\mathbb{Q})$, let $\mathscr{R}$ be a set of representatives of right cosets of the subgroup $\mathcal{Z}(\sigma)\,\mathrm{Gal}(\mathbb{L}/\mathbb{K})$ in $\mathrm{Gal}(\mathbb{L}/\mathbb{Q})$. Then $\mathscr{C}$ is the disjoint union

$$\mathscr{C} = \bigcup_{\nu\in\mathscr{R}} C_\nu, \tag{3·17}$$

where C_ν is the conjugacy class of $\nu\sigma\nu^{-1}$ in $\mathrm{Gal}(\mathbb{L}/\mathbb{K})$. If $\mathfrak{p}_1, \ldots, \mathfrak{p}_{[\mathbb{K}:\mathbb{Q}]}$ are linear prime ideals of $\mathbb{K}$ lying over the same prime p, unramified in $\mathbb{L}$, one can easily verify (see e.g. [**17**, p. 126f]) the equivalence

$$\exists i : \left[\frac{\mathbb{L}\mid\mathbb{K}}{\mathfrak{p}_i}\right] = C \Longleftrightarrow \left[\frac{\mathbb{L}\mid\mathbb{Q}}{p}\right] = \mathscr{C}.$$

In this case we deduce from (3·17) that the number of such prime ideals is exactly $|C|[\mathbb{K}:\mathbb{Q}]/|\mathscr{C}|$. Thus we obtain

$$\sum_{\mathfrak{p}\in\mathcal{P}_C(x,\mathbb{L}/\mathbb{K})} \mathcal{I}_\gamma^\kappa(\mathfrak{p}) = \frac{|C|[\mathbb{K}:\mathbb{Q}]}{|\mathscr{C}|} \sum_{p\in\mathcal{P}_{\mathscr{C}}(x,\mathbb{L}/\mathbb{Q})} \mathcal{I}_\gamma^\kappa(p) + O_{\mathbb{K}}(x^{2/3}). \tag{3·18}$$

In case $\gamma > \kappa$, combining (3·18) with the observation (3·14) made at the end of Section 3·1 yields

$$\sum_{\mathfrak{p}\in\mathcal{P}_C(x,\mathbb{L}/\mathbb{K})} \mathcal{I}_\gamma^\kappa(\mathfrak{p}) = \mathrm{li}(x)[\mathbb{K}:\mathbb{Q}] \sum_{n\geqslant 1} \frac{c_C(n)\varphi_\kappa(n)}{n^{\gamma-\kappa+1}[\mathbb{L}(\zeta_n):\mathbb{Q}]} + O\left(\frac{\mathrm{li}(x)}{(\log x)^{\frac{\gamma(\gamma-\kappa)}{6\gamma-3\kappa}-\varepsilon}}\right), \tag{3·19}$$

since $c_{\mathscr{C}}(n) = (|\mathscr{C}|/|C|)c_C(n)$, as one can easily derive from Lemma 7. The implied constant in (3·19) depends on γ, κ, $\mathbb{L}$ and ε. Let us now consider the case $\gamma = \kappa$ and postpone the computation of the sum in (3·19). In that case (3·2) yields

$$\sum_{p\in\mathcal{P}_{\mathscr{C}}(x,\mathbb{L}/\mathbb{Q})} \mathcal{I}_\gamma^\gamma(p) = \sum_{p\in\mathcal{P}_{\mathscr{C}}(x,\mathbb{L}/\mathbb{Q})} \sum_{d\mid p-1} \sum_{f\mid(p-1)/d} \frac{\mu(f)}{f^\gamma}.$$

Here the terms for large d cannot be neglected any more. Let $y = \log^2 x$, and recall that $\gamma \geqslant 1$. Rearranging summation we obtain

$$\begin{aligned}\sum_{p\in\mathcal{P}_{\mathscr{C}}(x,\mathbb{L}/\mathbb{Q})} \mathcal{I}_\gamma^\gamma(p) &= \sum_{f\leqslant x} \frac{\mu(f)}{f^\gamma} \sum_{\substack{p\in\mathcal{P}_{\mathscr{C}}(x,\mathbb{L}/\mathbb{Q})\\ f\mid p-1}} \sum_{d\mid\frac{p-1}{f}} 1 \\ &= \sum_{f\leqslant y} \frac{\mu(f)}{f^\gamma} \sum_{\substack{p\in\mathcal{P}_{\mathscr{C}}(x,\mathbb{L}/\mathbb{Q})\\ f\mid p-1}} \sum_{d\mid\frac{p-1}{f}} 1 + O\left(\frac{x}{\log x}\right),\end{aligned}$$

by the same arguments used in the proof of Lemma 6, and

$$\sum_{n\leqslant x} \frac{1}{\varphi(n)} = O(\log x) \tag{3·20}$$

(cf. Lemma 15). Using the classical estimate

$$\sum_{d\mid n} 1 = 2\sum_{\substack{d\mid n\\ d<\sqrt{n}}} 1 + O(1)$$

and the Brun–Titchmarsh inequality we get

$$\sum_{p\in\mathcal{P}_{\mathscr{C}}(x,\mathbb{L}/\mathbb{Q})} \mathcal{I}_{\gamma}^{\gamma}(p) = 2\sum_{f\leqslant y}\frac{\mu(f)}{f^{\gamma}} \sum_{\substack{p\in\mathcal{P}_{\mathscr{C}}(x,\mathbb{L}/\mathbb{Q})\\ f\mid p-1}} \sum_{\substack{d\mid \frac{p-1}{f}\\ d<\sqrt{\frac{p-1}{f}}}} 1 + O\left(\frac{x}{\log x}\right).$$

The above error term could be improved for $\gamma > 1$. Since there occur larger error terms in the sequel, however, we neglect this precision. Now we rearrange the sum again and get

$$\sum_{p\in\mathcal{P}_{\mathscr{C}}(x,\mathbb{L}/\mathbb{Q})} \mathcal{I}_{\gamma}^{\gamma}(p) = 2\sum_{f\leqslant y}\frac{\mu(f)}{f^{\gamma}} \sum_{d<\sqrt{\frac{x}{f}}} \sum_{\substack{p\in\mathcal{P}_{\mathscr{C}}(x,\mathbb{L}/\mathbb{Q})\\ p>d^2f+1\\ df\mid p-1}} 1 + O\left(\frac{x}{\log x}\right).$$

By the Brun–Titchmarsh inequality and (3·20) one easily deduces

$$\sum_{f\leqslant y}\frac{\mu(f)}{f^{\gamma}} \sum_{d<\sqrt{\frac{x}{f}}} \sum_{\substack{p\in\mathcal{P}_{\mathscr{C}}(d^2f,\mathbb{L}/\mathbb{Q})\\ df\mid p-1}} 1 = O\left(\frac{x}{\log x}\right).$$

Let now B be a positive parameter. Proceeding as before we get rid of the terms with $\sqrt{x}/\log^{B} x \leqslant df < \sqrt{xf}$ and obtain

$$\sum_{p\in\mathcal{P}_{\mathscr{C}}(x,\mathbb{L}/\mathbb{Q})} \mathcal{I}_{\gamma}^{\gamma}(p) = 2\sum_{f\leqslant y}\frac{\mu(f)}{f^{\gamma}} \sum_{df<\frac{\sqrt{x}}{\log^{B} x}} \sum_{\substack{p\in\mathcal{P}_{\mathscr{C}}(x,\mathbb{L}/\mathbb{Q})\\ df\mid p-1}} 1 + O\left(\frac{x\log\log x}{\log x}\right). \tag{3·21}$$

Due to the large moduli df in (3·21), Proposition 8 is not applicable to estimate the right-hand side of (3·21) and Proposition 11 is not strong enough in general. Thus we assume the GRH for the fields $\mathbb{L}_{df}$ and apply the following result due to Lagarias and Odlyzko [**14**].

PROPOSITION 12 (Lagarias–Odlyzko). *Let $\mathbb{L}'/\mathbb{K}'$ be an arbitrary normal extension of number fields and $C' \subset \mathrm{Gal}(\mathbb{L}'/\mathbb{K}')$ a conjugacy class or empty. If the GRH for $\mathbb{L}'$ holds true, then*

$$\left|\pi_{C'}(x,\mathbb{L}'/\mathbb{K}') - \frac{|C'|}{[\mathbb{L}':\mathbb{K}']}\,\mathrm{li}(x)\right| \ll \frac{|C'|}{[\mathbb{L}':\mathbb{K}']}x^{1/2}\log\left(\Delta_{\mathbb{L}'}x^{[\mathbb{L}':\mathbb{Q}]}\right) + \log(\Delta_{\mathbb{L}'})$$

holds for every $x > 2$, where the implied constant is absolute.

By Proposition 12, Lemma 7 and Lemma 10, or by Proposition 11 if applicable, we find

$$\sum_{p\in\mathcal{P}_{\mathscr{C}}(x,\mathbb{L}/\mathbb{Q})} \mathcal{I}_{\gamma}^{\gamma}(p) = \frac{2|\mathscr{C}|}{|C|}\,\mathrm{li}(x)\sum_{f\leqslant y}\frac{\mu(f)}{f^{\gamma}} \sum_{df<\frac{\sqrt{x}}{\log^{B} x}} \frac{c_C(df)}{[\mathbb{L}_{df}:\mathbb{Q}]} + E + O\left(\frac{x\log\log x}{\log x}\right) \tag{3·22}$$

with

$$E \ll \sum_{f\leqslant y}\frac{1}{f^{\gamma}}\sum_{e<\frac{\sqrt{x}}{\log^{B}x}}\left[\frac{c_C(e)}{[\mathbb{L}_e:\mathbb{Q}]}x^{\frac{1}{2}}\log\left(\Delta_{\mathbb{L}_e}x^{[\mathbb{L}_e:\mathbb{Q}]}\right)+\log(\Delta_{\mathbb{L}_e})\right] \tag{3·23}$$

$$\ll_{\mathbb{L}} \log\log x\sum_{e<\frac{\sqrt{x}}{\log^{B}x}}\left[x^{\frac{1}{2}}\log(x)+[\mathbb{L}_e:\mathbb{Q}]\log(x)\right]\ll\frac{x\log\log x}{(\log x)^{B-1}}.$$

Choosing $B\geqslant 2$ we finally arrive at

$$\begin{aligned}\sum_{p\in\mathcal{P}_{\mathscr{C}}(x,\mathbb{L}/\mathbb{Q})}\mathcal{I}_{\gamma}^{\gamma}(p) &= \frac{2|\mathscr{C}|}{|C|}\operatorname{li}(x)\sum_{f\leqslant y}\frac{\mu(f)}{f^{\gamma}}\sum_{df<\frac{\sqrt{x}}{\log^{B}x}}\frac{c_C(df)}{[\mathbb{L}_{df}:\mathbb{Q}]}+O_{\mathbb{L}}\left(\frac{x\log\log x}{\log x}\right)\\ &= \frac{2|\mathscr{C}|}{|C|}\operatorname{li}(x)\sum_{f\geqslant 1}\frac{\mu(f)}{f^{\gamma}}\sum_{df<\frac{\sqrt{x}}{\log^{B}x}}\frac{c_C(df)}{[\mathbb{L}_{df}:\mathbb{Q}]}+O_{\mathbb{L}}\left(\frac{x\log\log x}{\log x}\right)\\ &= \frac{2|\mathscr{C}|}{|C|}\operatorname{li}(x)\sum_{n\leqslant\frac{\sqrt{x}}{\log^{B}x}}\frac{c_C(n)\varphi_{\gamma}(n)}{n[\mathbb{L}_n:\mathbb{Q}]}+O_{\mathbb{L}}\left(\frac{x\log\log x}{\log x}\right)\\ &= \frac{2|\mathscr{C}|}{|C|}\operatorname{li}(x)\sum_{n\leqslant\sqrt{x}}\frac{c_C(n)\varphi_{\gamma}(n)}{n[\mathbb{L}_n:\mathbb{Q}]}+O_{\mathbb{L}}\left(\frac{x\log\log x}{\log x}\right).\end{aligned} \tag{3·24}$$

In the light of (3·19) and (3·24) it suffices to compute an asymptotic formula for the sum

$$\sum_{n\leqslant\sqrt{x}}\frac{c_C(n)\varphi_{\kappa}(n)}{n^{\gamma-\kappa+1}[\mathbb{L}_n:\mathbb{Q}]}$$

with arbitrary $\gamma\geqslant\kappa$ to prove both, Theorem 4 (i) and (ii). Choosing a positive integer m such that $\mathbb{L}^{ab}\subset\mathbb{Q}(\zeta_m)$, we obtain

$$\begin{aligned}\sum_{n\leqslant\sqrt{x}}\frac{c_C(n)\varphi_{\kappa}(n)}{n^{\gamma-\kappa+1}[\mathbb{L}(\zeta_n):\mathbb{Q}]} &= \sum_{d|m}\sum_{\substack{n\leqslant\sqrt{x}\\(n,m)=d}}\frac{c_C(n)\varphi_{\kappa}(n)[\mathbb{L}\cap\mathbb{Q}(\zeta_n):\mathbb{Q}]}{n^{\gamma-\kappa+1}\varphi(n)[\mathbb{L}:\mathbb{Q}]}\\ &= \frac{|C|}{[\mathbb{L}:\mathbb{Q}]}\sum_{\substack{d|m\\c_C(d)\neq 0}}[\mathbb{L}\cap\mathbb{Q}(\zeta_d):\mathbb{Q}]\sum_{\substack{n\leqslant\sqrt{x}\\(n,m)=d}}\frac{\varphi_{\kappa}(n)}{n^{\gamma-\kappa+1}\varphi(n)}\end{aligned}$$

since $\mathbb{Q}(\zeta_k)\cap\mathbb{Q}(\zeta_l)=\mathbb{Q}(\zeta_{(k,l)})$. The subsequent lemma eventually completes the proof in case $\gamma\geqslant\kappa$ as the obtained sum on d is positive, since all summands are non-negative, and the term associated to $d=1$ is not zero. As in Section 3·1 the case $\gamma<\kappa$ again follows by swapping γ and κ and applying a simple partial summation argument.

LEMMA 13. *Let $\gamma\geqslant 1$ be an integer, and $\kappa>0$ a real number satisfying $\gamma\geqslant\kappa$. For any two positive integers m, d with $d\mid m$ we define $a_{\gamma}^{\kappa}(m,d)$ to be the product*

$$\prod_{p\nmid m}\left(1+\frac{1-p^{1-\kappa}}{(p-1)p^{\gamma-\kappa+1}}\right)\prod_{p|d}\left(1+\frac{1-p^{1-\kappa}}{(p-1)p^{\gamma-\kappa}}\right)\prod_{\substack{p|\frac{m}{d}\\p\nmid d}}\left(1+\frac{(1-p^{1-\kappa})(p^{\gamma-\kappa}-1)}{(p-1)p^{\gamma-\kappa}(p^{\gamma-\kappa+1}-1)}\right).$$

This product is absolutely convergent and positive. If $\gamma = \kappa$, we have

$$\sum_{\substack{n\leqslant x\\(n,m)=d}} \frac{\varphi_\kappa(n)}{n^{\gamma-\kappa+1}\varphi(n)} = \frac{\varphi_{\gamma-\kappa+1}(\frac{m}{d})a_\gamma^\kappa(m,d)}{md^{\gamma-\kappa}}\log x + O_m(1),$$

and, if $\gamma > \kappa$, then

$$\sum_{\substack{n\leqslant x\\(n,m)=d}} \frac{\varphi_\kappa(n)}{n^{\gamma-\kappa+1}\varphi(n)} = \frac{\varphi_{\gamma-\kappa+1}(\frac{m}{d})a_\gamma^\kappa(m,d)\zeta(\gamma-\kappa+1)}{md^{\gamma-\kappa}} + O_{m,\gamma,\kappa}(x^{\kappa-\gamma}).$$

Proof. By Möbius inversion we initially obtain

$$\sum_{\substack{n\leqslant x\\(n,m)=d}} \frac{\varphi_\kappa(n)}{n^{\gamma-\kappa+1}\varphi(n)} = \sum_{e\mid\frac{m}{d}}\mu(e)\sum_{\substack{n\leqslant x\\ed\mid n}} \frac{\varphi_\kappa(n)}{n^{\gamma-\kappa+1}\varphi(n)}. \tag{3·25}$$

The function $\varphi_\kappa(n)/\varphi(n)$ is clearly multiplicative and may be written as

$$\frac{\varphi_\kappa(n)}{\varphi(n)} = \sum_{s\mid n}\mu^2(s)\xi_\kappa(s) \tag{3·26}$$

with a multiplicative function $\xi_\kappa(s)$ which fulfils

$$\xi_\kappa(p) = \frac{1-p^{1-\kappa}}{p-1} \tag{3·27}$$

for any prime p. Note that

$$|\xi_\kappa(p)| \leqslant \begin{cases} \frac{1}{\varphi(p)}, & \text{if } \kappa \geqslant 1,\\ 1, & \text{otherwise}\end{cases} \tag{3·28}$$

holds for all all primes p. By (3·26) the right-hand side of (3·25) equals

$$\frac{1}{d^{\gamma-\kappa+1}}\sum_{e\mid\frac{m}{d}}\frac{\mu(e)}{e^{\gamma-\kappa+1}}\sum_{s\leqslant x}\frac{\mu^2(s)\xi_\kappa(s)(s,ed)}{s^{\gamma-\kappa+1}}\sum_{n\leqslant\frac{x}{[s,ed]}}\frac{1}{n^{\gamma-\kappa+1}}.$$

As one can easily verify using (3·28), the sum on n may be extended to all $n\in\mathbb{N}$ if $\gamma>\kappa$, and to $n\leqslant x$ if $\kappa=\gamma$, which effects the asserted error terms. In both cases the sum on n thereby becomes independent of the other terms and yields the respective factors $\zeta(\gamma-\kappa+1)$ and $\log x$ in the assertion. By analogue arguments one may extend the sum on s to all $s\in\mathbb{N}$. Thus it remains to compute

$$\sum_{e\mid\frac{m}{d}}\frac{\mu(e)}{e^{\gamma-\kappa+1}}\sum_{s\geqslant 1}\frac{\mu^2(s)\xi_\kappa(s)(s,ed)}{s^{\gamma-\kappa+1}}. \tag{3·29}$$

The sum on s can be expressed as an Euler product, so that (3·29) becomes

$$\begin{aligned}&\sum_{e\mid\frac{m}{d}}\frac{\mu(e)}{e^{\gamma-\kappa+1}}\prod_{p\mid ed}\left(1+\frac{\xi_\kappa(p)}{p^{\gamma-\kappa}}\right)\prod_{p\nmid ed}\left(1+\frac{\xi_\kappa(p)}{p^{\gamma-\kappa+1}}\right) \\ &\quad=\prod_{p\nmid d}\left(1+\frac{\xi_\kappa(p)}{p^{\gamma-\kappa+1}}\right)\prod_{p\mid d}\left(1+\frac{\xi_\kappa(p)}{p^{\gamma-\kappa}}\right)\sum_{e\mid\frac{m}{d}}\frac{\mu(e)}{e^{\gamma-\kappa+1}}\prod_{\substack{p\mid e\\p\nmid d}}\left(\frac{1+\frac{\xi_\kappa(p)}{p^{\gamma-\kappa}}}{1+\frac{\xi_\kappa(p)}{p^{\gamma-\kappa+1}}}\right).\end{aligned} \tag{3·30}$$

The sum on e is clearly multiplicative, and equals

$$\prod_{\substack{p\mid\frac{m}{d}\\ p\mid d}}\left(1-\frac{1}{p^{\gamma-\kappa+1}}\right)\prod_{\substack{p\mid\frac{m}{d}\\ p\nmid d}}\left(1-\frac{1+\frac{\xi_\kappa(p)}{p^{\gamma-\kappa}}}{p^{\gamma-\kappa+1}+\xi_\kappa(p)}\right). \tag{3·31}$$

Combining (3·30) and (3·31) one easily checks that (3·29) equals

$$\prod_{p\nmid m}\left(1+\frac{\xi_\kappa(p)}{p^{\gamma-\kappa+1}}\right)\prod_{p\mid d}\left(1+\frac{\xi_\kappa(p)}{p^{\gamma-\kappa}}\right)\prod_{p\mid\frac{m}{d}}\left(1-\frac{1}{p^{\gamma-\kappa+1}}\right)\prod_{\substack{p\mid\frac{m}{d}\\ p\nmid d}}\left(1+\frac{\xi_\kappa(p)(p^{\gamma-\kappa}-1)}{p^{\gamma-\kappa}(p^{\gamma-\kappa+1}-1)}\right).$$

By (3·28) this product is positive, and inserting (3·27) yields the assertion.

4. *Averaging over all ideals*

4·1. *Proof of Theorem* 1

For an ideal $\mathfrak{a}$ of $\mathbb{K}$ let $\varphi(\mathfrak{a})$ and $\lambda(\mathfrak{a})$ denote order and exponent of $(\mathcal{O}_{\mathbb{K}}\,/\,\mathfrak{a})^*$, respectively. As in the classical case $\varphi(\mathfrak{a})$ is multiplicative on ideals by the Chinese Remainder Theorem and satisfies

$$\varphi(\mathfrak{a})=\mathcal{N}\mathfrak{a}\prod_{\mathfrak{p}\mid\mathfrak{a}}\left(1-\frac{1}{\mathcal{N}\mathfrak{p}}\right). \tag{4·1}$$

As for $\lambda(\mathfrak{a})$ we have

$$\lambda(\mathfrak{a})=\operatorname{lcm}(\varphi(\mathfrak{p}):\mathfrak{p}\mid\mathfrak{a}) \tag{4·2}$$

if $\mathfrak{a}$ is composed of distinct prime ideals. For an ideal $\mathfrak{a}$ which is divisible by the square of some prime ideal the situation is more complicated, for it depends on the inertia degree of $\mathfrak{p}$ over $\mathbb{Q}$ whether or not $(\mathcal{O}_{\mathbb{K}}\,/\,\mathfrak{p}^k)^*$ is cyclic for $k>1$ (cf. [**22**, p. 268]). One clearly has the trivial lower bound

$$\operatorname{ind}_\Gamma(\mathfrak{a})\gg_{\mathbb{K}}\frac{\varphi(\mathfrak{a})}{\lambda(\mathfrak{a})^\gamma}. \tag{4·3}$$

The implied constant accounts for the torsion part of Γ, and depends only on $\mathbb{K}$. Hence, to obtain a lower bound for κ-th moments of $\operatorname{ind}_\Gamma(\mathfrak{a})$, it suffices to establish one for the average order of $\varphi(\mathfrak{a})^\kappa/\lambda(\mathfrak{a})^{\gamma\kappa}$ over ideals $\mathfrak{a}$ which satisfy $\overline{\Gamma}\subset(\mathcal{O}_{\mathbb{K}}\,/\,\mathfrak{a})^*$. In this regard we state the following number field analogue of a statement of Luca and Sankaranarayanan [**18**].

PROPOSITION 14. *Let $\mathbb{K}$ be a number field and Γ a finitely generated subgroup of $\mathbb{K}^*$ of rank $\gamma\geqslant 1$. For any $\kappa>0$, any $r>0$ and any $\delta>0$ which is admissible in the sense of Theorem* 1 *we have*

$$\sum_{\substack{\mathcal{N}\mathfrak{a}\leqslant x\\ \overline{\Gamma}\subset(\mathcal{O}_{\mathbb{K}}\,/\,\mathfrak{a})^*}}\frac{\varphi(\mathfrak{a})^\kappa}{\lambda(\mathfrak{a})^r}\gg x^{1+\kappa-\delta+o(1)},$$

where the implied constant depends on κ, γ, r and $\mathbb{K}$.

Proposition 14 is proved by a simple number field adaption of the original proof in [**18**]. In fact, it suffices to replace primes by prime ideals $\mathfrak{p}$ of $\mathbb{K}$ satisfying $\overline{\Gamma}\subset(\mathcal{O}_{\mathbb{K}}\,/\,\mathfrak{p})^*$ therein, and utilise (4·1), (4·2) and $\varphi(\mathfrak{a})\geqslant\varphi(\mathcal{N}\mathfrak{a})\gg\mathcal{N}\mathfrak{a}/\log\log\mathcal{N}\mathfrak{a}$ (cf. [**28**, p. 84]).

4·2. *Proof of Theorem* 2

We will now verify the admissible values for δ asserted in Theorem 2. Our proof combines ideas of [**2**] and [**8**]. In the sequel $\mathbb{L}$ will denote $\mathbb{Q}(\zeta_m)$ if $\mathbb{K}^{(n)}$ is abelian and contained in $\mathbb{Q}(\zeta_m)$. Otherwise we set $\mathbb{L} = \mathbb{K}^{(n)}$. A prime number which splits completely in $\mathbb{L}$ necessarily lifts to linear prime ideals in $\mathbb{K}$. Hence

$$\begin{aligned}\sharp\,\mathcal{P}_{\delta,\mathbb{K}}(y) &\geqslant \sharp\left\{\mathfrak{p}\ \text{linear} : \mathcal{N}\mathfrak{p} \leqslant y,\ P^+(\mathcal{N}\mathfrak{p}-1) < y^\delta\right\}\\ &\geqslant \sharp\left\{p \leqslant y : p \text{ splits completely in } \mathbb{L},\ P^+(p-1) < y^\delta\right\}. \qquad (4{\cdot}4)\end{aligned}$$

Proceeding as in the original work of Balog [**2**], we let $\varepsilon > 0$ be sufficiently small and define

$$g(p) := \sharp\{p-1 = kn : P^+(kn) \leqslant y^\delta,\ N_1 < n \leqslant N_2\}$$

with

$$N_1 = y^{\frac{1}{2}+\varepsilon} \qquad \text{and} \qquad N_2 = y^{\frac{1}{2}+2\varepsilon}.$$

Then (4·4) and the Cauchy–Schwarz inequality yield

$$\sharp\,\mathcal{P}_{\delta,\mathbb{K}}(y) \geqslant \Bigg(\sum_{p\in\mathcal{P}_C(y,\mathbb{L}/\mathbb{Q})} g(p)\Bigg)^2 \Bigg(\sum_{p\in\mathcal{P}_C(y,\mathbb{L}/\mathbb{Q})} g(p)^2\Bigg)^{-1}, \qquad (4{\cdot}5)$$

where $C = \{\mathrm{id}\} \subset \mathrm{Gal}(\mathbb{L}/\mathbb{Q})$ and $\mathcal{P}_C(y, \mathbb{L}/\mathbb{Q})$ is defined as in Section 2·2. Thus we need a good lower and upper bound for the numerator and the denominator, respectively.

As for the denominator the Brun–Titchmarsh inequality yields

$$\begin{aligned}\sum_{p\in\mathcal{P}_C(y,\mathbb{L}/\mathbb{Q})} g(p)^2 &\leqslant \sum_{p\leqslant y}\Bigg(\sum_{\substack{k\mid p-1\\ k\leqslant(y-1)/N_1}} 1\Bigg)^2 \leqslant \sum_{k_1,k_2\leqslant\frac{y-1}{N_1}} \pi(y;1,[k_1,k_2])\\ &\ll \frac{y}{\log y}\sum_{k_1,k_2\leqslant\frac{y-1}{N_1}} \frac{1}{\varphi([k_1,k_2])}.\end{aligned}$$

By (3·20) we obtain

$$\sum_{a,b\leqslant z}\frac{1}{\varphi([a,b])} \leqslant \sum_{\substack{a,b,c\leqslant z\\ (a,b)=c}} \frac{1}{\varphi\left(\frac{a}{c}\right)\varphi\left(\frac{b}{c}\right)\varphi(c)} \leqslant \Bigg(\sum_{n\leqslant z}\frac{1}{\varphi(n)}\Bigg)^3 \ll \log^3 z$$

and hence

$$\sum_{p\in\mathcal{P}_C(y,\mathbb{L}/\mathbb{Q})} g(p)^2 \ll y\log^2 y. \qquad (4{\cdot}6)$$

As for the numerator we clearly have

$$\begin{aligned}g(p) &= \sharp\{p-1 = kn : P^+(k) \leqslant y^\delta,\ N_1 < n \leqslant N_2\} -\\ &\qquad \sharp\{p-1 = kn : P^+(k) \leqslant y^\delta,\ P^+(n) > y^\delta,\ N_1 < n \leqslant N_2\}\\ &\geqslant \sharp\{p-1 = kn : P^+(k) \leqslant y^\delta,\ N_1 < n \leqslant N_2\} -\\ &\qquad \sharp\{p-1 = kql : y^\delta < q,\ N_1 < ql \leqslant N_2\},\end{aligned}$$

where the letter q is reserved for primes. Hence

$$\sum_{p\in\mathcal{P}_C(y,\mathbb{L}/\mathbb{Q})} g(p) \geqslant S_1 - S_2$$

with

$$S_1 = \sum_{\substack{k\leqslant y\\ P^+(k)\leqslant y^\delta}} \sum_{\substack{p\in\mathcal{P}_C(y,\mathbb{L}/\mathbb{Q})\\ k|p-1\\ N_1<\frac{p-1}{k}\leqslant N_2}} 1 \qquad \text{and} \qquad S_2 = \sum_{y^\delta<q} \sum_{N_1<ql\leqslant N_2} \sum_{\substack{p\in\mathcal{P}_C(y,\mathbb{L}/\mathbb{Q})\\ ql|p-1}} 1.$$

4·2·1. *The sum S_1*

We must establish a lower bound for S_1. We do so in detail for part (i) and (ii) of Theorem 2 and briefly discuss the case (iii) at the end of Section 4·2·2. To start with we observe that

$$S_1 \geqslant \sum_{\substack{\frac{y}{N_2}<k\leqslant\frac{y}{N_1}\\ P^+(k)\leqslant y^\delta}} \sum_{\substack{p\in\mathcal{P}_C(y,\mathbb{L}/\mathbb{Q})\\ p>N_1k+1\\ k|p-1}} 1 = \sum_{\substack{\frac{y}{N_2}<k\leqslant\frac{y}{N_1}\\ P^+(k)\leqslant y^\delta}} \sum_{\substack{p\in\mathcal{P}_C(y,\mathbb{L}/\mathbb{Q})\\ k|p-1}} 1 + O\left(\frac{y}{\log y}\right)$$

holds by the Brun–Titchmarsh inequality, since

$$\sum_{\substack{\frac{y}{N_2}<k\leqslant\frac{y}{N_1}\\ P^+(k)\leqslant y^\delta}} \sum_{\substack{p\in\mathcal{P}_C(y,\mathbb{L}/\mathbb{Q})\\ p\leqslant N_1k+1\\ k|p-1}} 1 \leqslant \sum_{k\leqslant\frac{y}{N_1}} \pi(N_1k+1;1,k) \ll \frac{N_1}{\log y}\sum_{k\leqslant\frac{y}{N_1}}\frac{k}{\varphi(k)} \ll \frac{y}{\log y}.$$

Invoking Proposition 12 we find

$$S_1 \geqslant \operatorname{li}(y) \sum_{\substack{\frac{y}{N_2}<k\leqslant\frac{y}{N_1}\\ P^+(k)\leqslant y^\delta}} \frac{1}{[\mathbb{L}(\zeta_k):\mathbb{Q}]} + O_{\mathbb{K}}\left(\frac{y}{\log y}\right). \tag{4·7}$$

If $\mathbb{L}=\mathbb{Q}(\zeta_m)$, the same follows by the classical Bombieri–Vinogradov Theorem, since we have $\pi_C(y,\mathbb{L}/\mathbb{Q}) = \pi(y;1,m)$ in this case. Letting $m'\in\mathbb{N}$ satisfy $\mathbb{L}^{ab}\subset\mathbb{Q}(\zeta_{m'})$ we deduce

$$S_1 \geqslant \operatorname{li}(y)\sum_{d|m'}\frac{1}{[\mathbb{L}:\mathbb{L}\cap\mathbb{Q}(\zeta_d)]} \sum_{\substack{\frac{y}{N_2}<k\leqslant\frac{y}{N_1}\\ (k,m')=d\\ P^+(k)\leqslant y^\delta}} \frac{1}{\varphi(k)} + O_{\mathbb{K}}\left(\frac{y}{\log y}\right) \tag{4·8}$$

by the same arguments as in Section 3·3. The sum over k is bounded from below by

$$\sum_{\substack{\frac{y}{N_2}<k\leqslant\frac{y}{N_1}\\ (k,m')=d}} \frac{1}{\varphi(k)} - \sum_{y^\delta<q\leqslant y^{1/2}} \frac{1}{\varphi(q)} \sum_{\substack{\frac{y}{qN_2}<l\leqslant\frac{y}{qN_1}\\ (l,m')=d}} \frac{1}{\varphi(l)} \tag{4·9}$$

if we choose y big enough so that (ql,m') becomes (l,m'). To treat sums of this type we apply the following elementary result which may be obtained by the same arguments used in the proof of Lemma 13.

LEMMA 15. *For positive integers $l \mid k$ let*

$$b(k,l) := \frac{\varphi(\frac{k}{l})l}{\varphi(l)k}\prod_{p\nmid k}\left(1+\frac{1}{p(p-1)}\right).$$

Then

$$\sum_{\substack{n\leqslant x\\ (k,n)=l}} \frac{1}{\varphi(n)} = b(k,l)\log x + O_k(1).$$

Combining this result with (4·8), (4·9) and Mertens' Formula [**28**, p. 16] we finally infer

$$S_1 \geqslant \mathrm{li}(y)\log\left(\frac{N_2}{N_1}\right)\left(1-\log\left(\frac{1}{2\delta}\right)\right)\sum_{d\mid m'}\frac{b(m',d)}{[\mathbb{L}:\mathbb{L}\cap\mathbb{Q}(\zeta_d)]}+O_{\mathbb{K}}\left(\frac{y\log\log y}{\log y}\right). \quad (4{\cdot}10)$$

4·2·2. *The sum S_2*

To estimate S_2 we must handle sums of $\pi(x;a,q)$ for q slightly exceeding $x^{1/2}$. In this case the Bombieri–Vinogradov Theorem is not applicable and the Brun–Titchmarsh inequality is too imprecise. To this end we state the following result of Bombieri, Friedlander and Iwaniec [**4**] which represents a continuous transition between these two statements.

PROPOSITION 16 (Bombieri–Friedlander–Iwaniec). *Let $a \neq 0$ be an integer, $A > 0$ and $2 \leqslant Q \leqslant x^{3/4}$. Let $\mathcal{Q}$ consist of all $q \in \mathbb{N}$, prime to a, from an interval $Q' < q \leqslant Q$. Then*

$$\sum_{q\in\mathcal{Q}}\left|\pi(x;a,q)-\frac{\mathrm{li}(x)}{\varphi(q)}\right|$$
$$\leqslant\left[L\left(\theta-\frac{1}{2}\right)^2\frac{x}{\log x}+O_A\left(\frac{x\log^3\log x}{\log^3 x}\right)\right]\sum_{q\in\mathcal{Q}}\frac{1}{\varphi(q)}+O_{a,A}\left(\frac{x}{\log^A x}\right),$$

where $\theta = \log Q/\log x$ and L is an absolute constant.

We treat the cases $\mathbb{L} = \mathbb{Q}(\zeta_m)$ and $\mathbb{L} = \mathbb{K}^{(n)}$ separately. If $\mathbb{L} = \mathbb{Q}(\zeta_m)$, then S_2 becomes

$$\sum_{y^\delta<q}\ \sum_{N_1<ql\leqslant N_2}\ \sum_{\substack{p\leqslant y\\ [m,ql]\mid p-1}} 1$$

and, for $\delta > 1/4+\varepsilon$, Proposition 16 and Lemma 15 yield

$$S_2 = \sum_{y^\delta<q\leqslant N_2}\ \sum_{\frac{N_1}{q}<l\leqslant\frac{N_2}{q}}\frac{\mathrm{li}(y)}{[\mathbb{L}(\zeta_{ql}):\mathbb{Q}]}+O(\varepsilon^2)\,\mathrm{li}(y)\sum_{N_1<k\leqslant N_2}\frac{1}{[\mathbb{L}(\zeta_k):\mathbb{Q}]}$$
$$\leqslant \mathrm{li}(y)\Bigg(\sum_{y^\delta<q\leqslant N_2}\frac{1}{\varphi(q)}\sum_{\frac{N_1}{q}<l\leqslant\frac{N_2}{q}}\frac{1}{[\mathbb{L}(\zeta_l):\mathbb{Q}]}+\log(N_2/N_1)O\left(\varepsilon^2\right)\Bigg).$$

Applying the same arguments as in the estimation of S_1 it is easily shown that

$$S_2 \leqslant \mathrm{li}(y)\log(N_2/N_1)\log\left(\frac{\frac{1}{2}+\varepsilon}{\delta}\right)\left(\sum_{d\mid m}\frac{b(m,d)}{[\mathbb{L}:\mathbb{L}\cap\mathbb{Q}(\zeta_d)]}+O\left(\varepsilon^2\right)\right). \quad (4{\cdot}11)$$

Now choose $m' = m$ in (4·10). Then, for $\delta > 1/(2\sqrt{e})$, we have $S_1 - S_2 \gg_{\mathbb{K}} y$ if y is large and ε small enough. This proves Theorem 2 (i).

Now assume that $\mathbb{L} = \mathbb{K}^{(n)}$ and is not contained in any cyclotomic field. Unfortunately the splitting condition $p \in \mathcal{P}_C(\mathbb{L}/\mathbb{Q})$ cannot be translated into an arithmetic progression condition if $\mathbb{K}^{(n)}$ is not abelian. Hence we omit this condition and start with the trivial estimate

$$S_2 \leqslant \sum_{y^\delta<q\leqslant N_2}\ \sum_{N_1<ql\leqslant N_2}\ \sum_{\substack{p\leqslant y\\ ql\mid p-1}} 1,$$

probably loosing a lot. As in the first case we invoke Proposition 16 and deduce

$$\begin{aligned} S_2 &\leqslant \mathrm{li}(y)\Bigg(\sum_{y^\delta<q\leqslant N_2}\frac{1}{\varphi(q)}\sum_{\frac{N_1}{q}<l\leqslant\frac{N_2}{q}}\frac{1}{\varphi(l)}+O(\varepsilon^2)\sum_{N_1<k\leqslant N_2}\frac{1}{\varphi(k)}\Bigg)\\ &\leqslant \mathrm{li}(y)\log(N_2/N_1)\log\left(\frac{\frac{1}{2}+\varepsilon}{\delta}\right)\big(b(1,1)+O(\varepsilon^2)\big), \end{aligned} \tag{4·12}$$

for $\delta > 1/4+\varepsilon$. Finally, by (4·10) and (4·12), we obtain $S_1 - S_2 \gg_{\mathbb{K}} y$ if

$$\delta > \frac{1}{2}\exp\left\{-\frac{\sum_{d|m'}\frac{b(m',d)}{[\mathbb{L}:\mathbb{L}\cap\mathbb{Q}(\zeta_d)]}}{b(1,1)+\sum_{d|m'}\frac{b(m',d)}{[\mathbb{L}:\mathbb{L}\cap\mathbb{Q}(\zeta_d)]}}\right\}$$

and y and ε are chosen large and small enough, respectively. Since $[\mathbb{L}:\mathbb{L}\cap\mathbb{Q}(\zeta_d)]\leqslant[\mathbb{L}:\mathbb{Q}]$ and $\sum_{d|m'}b(m',d)=b(1,1)$ we clearly have

$$\frac{\sum_{d|m'}\frac{b(m',d)}{[\mathbb{L}:\mathbb{L}\cap\mathbb{Q}(\zeta_d)]}}{b(1,1)+\sum_{d|m'}\frac{b(m',d)}{[\mathbb{L}:\mathbb{L}\cap\mathbb{Q}(\zeta_d)]}} \geqslant \frac{1}{[\mathbb{L}:\mathbb{Q}]+1}$$

and Theorem 2 (ii) follows. As for Theorem 2 (iii), we first observe that (4·7) remains true by Proposition 11, if we restrict to those k for which $\mathbb{Q}(\zeta_k)\cap\mathbb{L}=\mathbb{Q}$. If $(m',k)=d$ for some divisor d of m' we clearly have $\mathbb{Q}(\zeta_k)\cap\mathbb{L}=\mathbb{Q}(\zeta_d)\cap\mathbb{L}$. Hence, (4·8) holds if one restricts to divisors d of m' which satisfy $\mathbb{Q}(\zeta_d)\cap\mathbb{L}=\mathbb{Q}$. Proceeding as before in the cases (ii) and (iii) finally yields the choice

$$\delta_0=\frac{1}{2}\exp\left\{-\frac{\sum^*_{d|m'}b(m',d)}{b(1,1)[\mathbb{L}:\mathbb{Q}]+\sum^*_{d|m'}b(m',d)}\right\},$$

where * indicates the restriction to those d for which $\mathbb{Q}(\zeta_d)\cap\mathbb{L}=\mathbb{Q}$.

Acknowledgements. The author wants to thank the Volkswagen Foundation for their support, Valentin Blomer for fruitful discussions and pointing out the existence of the article [**18**] and David Rohrlich for helpful comments on earlier versions of this paper.

REFERENCES

[**1**] R. C. BAKER and G. HARMAN. Shifted primes without large prime factors. *Acta Arith.* **83** (1998), pp. 331–361.

[**2**] A. BALOG. $p+a$ without large prime factors. In *Seminar on Number Theory*, 1983–1984 (Talence, 1983/1984); (Université Bordeaux I, Talence, 1984), pp. Exp. No. 31, 5.

[**3**] V. BLOMER and F. BRUMLEY. On the Ramanujan conjecture over number fields. *Ann. of Math.* (2); **174** (2011), pp. 581–605.

[**4**] E. BOMBIERI, J. B. FRIEDLANDER and H. IWANIEC. Primes in arithmetic progressions to large moduli. III. *J. Amer. Math. Soc.* **2** (1989), pp. 215–224.

[**5**] P. ERDŐS and M. R. MURTY. On the order of $a \pmod p$), In *Number Theory* (Ottawa, ON, 1996). CRM Proc. Lecture Notes vol. 19 (Amer. Math. Soc. Providence, RI, 1999), pp. 87–97.

[**6**] A. T. FELIX. Generalizing the Titchmarsh divisor problem. *Int. J. Number Theory* **8** (2012), pp. 613–629.

[**7**] J. FRIEDLANDER and H. IWANIEC. *Opera de Cribro*. American Mathematical Society Colloquium Publications vol. 57. (American Mathematical Society, Providence, RI, 2010).

[**8**] J. B. FRIEDLANDER. Shifted primes without large prime factors. In *Number Theory and Applications* (Banff, AB, 1988). NATO Adv. Sci. Inst. Ser. C Math. Phys. Sci. vol. 265. (Kluwer Academic Published, Dordrecht, 1989), pp. 393–401.

[**9**] D. HILBERT. *The Theory of Algebraic Number Fields* (Springer-Verlag, Berlin, 1998).

[**10**] J. C. JANTZEN and J. SCHWERMER. *Algebra* (Springer-Verlag, Berlin, 2009).

[**11**] H. H. KIM. Functoriality for the exterior square of GL_4 and the symmetric fourth of GL_2. *J. Amer. Math. Soc.* **16** (2003), pp. 139–183 (electronic). With Appendix 1 by Dinakar Ramakrishnan and Appendix 2 by Kim and Peter Sarnak.

[**12**] P. KURLBERG. On the order of unimodular matrices modulo integers. *Acta Arith.* **110** (2003), pp. 141–151.

[**13**] P. KURLBERG and C. POMERANCE. On a problem of Arnold: the average multiplicative order of a given integer, *Algebra Number Theory* **7** (2013), pp. 981–999.

[**14**] 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) pp. 409–464.

[**15**] H. W. LENSTRA, JR. On Artin's conjecture and Euclid's algorithm in global fields. *Invent. Math.* **42** (1977), pp. 201–224.

[**16**] J. V. LINNIK. *The Dispersion Method in Binary Additive Problems*. Trans. by S. Schuur (American Mathematical Society, Providence, R.I., 1963).

[**17**] F. LORENZ. Algebraische Zahlentheorie (Bibliographisches Institut, Mannheim 1993).

[**18**] F. LUCA and A. SANKARANARAYANAN. On the moments of the Carmichael λ function. *Acta Arith.* **123** (2006), pp. 389–398.

[**19**] W. LUO, Z. RUDNICK and P. SARNAK. On the generalized Ramanujan conjecture for $\mathrm{GL}(n)$. In *Automorphic Forms, Automorphic Representations and Arithmetic* (Fort Worth, TX, 1996). Proc. Sympos. Pure Math. vol. 66. (Amer. Math. Soc. Providence, RI, 1999) pp. 301–310.

[**20**] M. R. MURTY and V. K. MURTY. A variant of the Bombieri–Vinogradov theorem. In *Number Theory* (Montreal, Que., 1985). CMS Conf. Proc. vol. 7 (Amer. Math. Soc. Providence, RI, 1987), pp. 243–272.

[**21**] M. R. MURTY and K. PETERSEN. A Bombieri–Vinogradov theorem for all number fields, *Trans. Amer. Math. Soc.* **365** (2013), pp. 4987–5032.

[**22**] W. NARKIEWICZ. Elementary and Analytic Theory of Algebraic Numbers. Springer Monogr. Math. (Springer-Verlag, Berlin, third ed., 2004).

[**23**] J. NEUKIRCH. Algebraische Zahlentheorie (Springer-Verlag, Berlin, 2007).

[**24**] D. E. ROHRLICH. Self-dual Artin representations. In *Automorphic Representations and L-functions*, vol. 22 (Tata Institute of Fundamental Research Studies in Mathematics, Mumbai, 2013), pp. 455–499.

[**25**] D. E. ROHRLICH. Nonvanishing of L-functions for GL(2). *Invent. Math.* **97** (1989), pp. 381–403.

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

[**27**] H. M. STARK. Some effective cases of the Brauer–Siegel theorem. *Invent. Math.* **23** (1974), pp. 135–152.

[**28**] G. TENENBAUM. *Introduction to Analytic and Probabilistic Number Theory*. Cambridge Studies in Advanced Math. vol. 46. (Cambridge University Press, Cambridge, 1995).

[**29**] S. S. WAGSTAFF, JR. Pseudoprimes and a generalization of Artin's conjecture. *Acta Arith.* **41**, pp. 141–150.

[**30**] L. C. WASHINGTON. Introduction to Cyclotomic Fields. Graduate Texts in Math. vol. 83. (Springer-Verlag, New York, second ed., 1997).

[**31**] J. ZELINSKY. Upper bounds for the number of primitive ray class characters with conductor below a given bound. arXiv:1307.2319 [math.NT].