Functiones et Approximatio
XXXIII (2005), 85–95

ON PRIMES p FOR WHICH d DIVIDES $\mathrm{ORD}_p(g)$

Pieter Moree

Abstract: Let $N_g(d)$ be the set of primes p such that the order of g modulo p, $\mathrm{ord}_p(g)$, is divisible by a prescribed integer d. Wiertelak showed that this set has a natural density, $\delta_g(d)$, with $\delta_g(d) \in \mathbb{Q}_{>0}$. Let $N_g(d)(x)$ be the number of primes $p \leqslant x$ that are in $N_g(d)$. A simple identity for $N_g(d)(x)$ is established. It is used to derive a more compact expression for $\delta_g(d)$ than known hitherto.

Keywords: multiplicative order, natural density.

1. Introduction

Let g be a rational number such that $g \notin \{-1,0,1\}$ (this assumption on g will be maintained throughout this note). Let $N_g(d)$ denote the set of primes p such that the order of $g(\mathrm{mod}\, p)$ is divisible by d (throughout the letter p will also be used to indicate primes). Let $N_g(d)(x)$ denote the number of primes in $N_g(d)$ not exceeding x. The quantity $N_g(d)(x)$ (and some variations of it) has been the subject of various publications [1, 3, 4, 7, 9, 11–19]. Hasse showed that $N_g(d)$ has a Dirichlet density in case d is an odd prime [3], respectively $d = 2$ [4]. The latter case is of additional interest since $N_g(2)$ is the set of prime divisors of the sequence $\{g^k + 1\}_{k=1}^{\infty}$. (One says that an integer divides a sequence if it divides at least one term of the sequence.) Wiertelak [12] established that $N_g(d)$ has a natural density $\delta_g(d)$ (around the same time Odoni [9] did so in the case d is a prime). In a later paper Wiertelak [15] proved, using sophisticated analytic tools, the following result (with $\mathrm{Li}(x)$ the logarithmic integral and with $\omega(d) = \sum_{p|d} 1$), which gives the best known error term to this date.

Theorem 1 [15]. *We have*

$$N_g(d)(x) = \delta_g(d)\mathrm{Li}(x) + O_{d,g}\left(\frac{x}{\log^3 x}(\log\log x)^{\omega(d)+1}\right).$$

Wiertelak also gave a formula for $\delta_g(d)$ which shows that this is always a positive rational number. A simpler formula for $\delta_g(d)$ (in case $g > 0$) has

2001 Mathematics Subject Classification: 11N37, 11R45

only recently been given by Pappalardi [10]. With some effort Pappalardi's and Wiertelak's expressions can be shown to be equivalent.

In this note a simple identity for $N_g(d)(x)$ will be established (given in Proposition 1). From this it is then inferred that $N_g(d)$ has a natural density $\delta_g(d)$ that is given by (4), which seems to be the simplest expression involving field degrees known for $\delta_g(d)$. This expression is then readily evaluated.

In order to state Theorem 2 some notation is needed. Write $g = \pm g_0^h$, where g_0 is positive and not an exact power of a rational and h as large as possible. Let $D(g_0)$ denote the discriminant of the field $\mathbb{Q}(\sqrt{g_0})$. The greatest common divisor of a and b respectively the lowest common multiple of a and b will be denoted by (a,b), respectively $[a,b]$. Given an integer d, we denote by d^∞ the supernatural number (sometimes called Steinitz number), $\prod_{p|d} p^\infty$. Note that $(v, d^\infty) = \prod_{p|d} p^{\nu_p(v)}$.

Definition. Let d be even and let $\epsilon_g(d)$ be defined as in Table 1 with $\gamma = \max\{0, \nu_2(D(g_0)/dh)\}$.

Table 1: $\epsilon_g(d)$

$g\backslash\gamma$	$\gamma=0$	$\gamma=1$	$\gamma=2$
$g>0$	$-1/2$	$1/4$	$1/16$
$g<0$	$1/4$	$-1/2$	$1/16$

Note that $\gamma \leqslant 2$. Also note that $\epsilon_g(d) = (-1/2)^{2^\gamma}$ if $g > 0$.

Theorem 2. *We have*

$$\delta_g(d) = \frac{\epsilon_1}{d(h, d^\infty)} \prod_{p|d} \frac{p^2}{p^2-1},$$

with

$$\epsilon_1 = \begin{cases} 1 & \text{if } 2 \nmid d; \\ 1 + 3(1-\mathrm{sgn}(g))(2^{\nu_2(h)}-1)/4 & \text{if } 2\|d \text{ and } D(g_0) \nmid 4d; \\ 1 + 3(1-\mathrm{sgn}(g))(2^{\nu_2(h)}-1)/4 + \epsilon_g(d) & \text{if } 2\|d \text{ and } D(g_0)|4d; \\ 1 & \text{if } 4|d,\ D(g_0) \nmid 4d; \\ 1 + \epsilon_{|g|}(d) & \text{if } 4|d,\ D(g_0)|4d. \end{cases}$$

In particular, if $g > 0$, then

$$\epsilon_1 = \begin{cases} 1 + (-1/2)^{2^{\max\{0,\nu_2(D(g_0)/dh)\}}} & \text{if } 2|d \text{ and } D(g_0)|4d; \\ 1 & \text{otherwise,} \end{cases}$$

and if h is odd, then

$$\epsilon_1 = \begin{cases} 1 + (-1/2)^{2^{\max\{0,\nu_2(D(g)/dh)\}}} & \text{if } 2|d \text{ and } D(g)|4d; \\ 1 & \text{otherwise,} \end{cases}$$

Using Proposition 1 of Section 2 it is also very easy to infer the following result, valid under the assumption of the Generalized Riemann Hypothesis (GRH).

Theorem 3. *Under GRH we have*

$$N_g(d)(x) = \delta_g(d)\mathrm{Li}(x) + O_{d,g}(\sqrt{x}\log^{\omega(d)+1} x),$$

where the implied constant depends at most on d and g.

In Tables 2 and 3 (Section 6) a numerical demonstration of Theorem 2 is given.

2. The key identity

Let $\pi_L(x)$ denote the number of unramified primes $p \leqslant x$ that split completely in the number field L. For integers $r|s$ let $K_{s,r} = \mathbb{Q}(\zeta_s, g^{1/r})$.

The starting point of the proof of Theorem 2 is the following proposition. By $r_p(g)$ the residual index of g modulo p is denoted (we have $r_g(p) = [\mathbb{F}_p : \langle g\rangle]$). Note that $\mathrm{ord}_p(g) r_p(g) = p-1$.

Proposition 1. *We have* $N_g(d)(x) = \sum_{v|d^\infty}\sum_{\alpha|d}\mu(\alpha)\pi_{K_{dv,\alpha v}}(x)$.

Proof. Let us consider the quantity $\sum_{\alpha|d}\mu(\alpha)\pi_{K_{dv,\alpha v}}(x)$. A prime p counted by this quantity satisfies $p \leqslant x$, $p \equiv 1(\mathrm{mod}\ dv)$ and $r_p(g) = vw$ for some integer w. Write $w = w_1 w_2$, with $w_1 = (w,d)$. Then the contribution of p to $\sum_{\alpha|d}\mu(\alpha)\pi_{K_{dv,\alpha v}}(x)$ is $\sum_{\alpha|w_1}\mu(\alpha)$. We conclude that

$$\sum_{\alpha|d}\mu(\alpha)\pi_{K_{dv,\alpha v}}(x) = \#\{p \leqslant x : p \equiv 1(\mathrm{mod}\ dv),\ v|r_p(g) \text{ and } (\frac{r_p(g)}{v}, d) = 1\}. \quad (1)$$

It suffices to show that

$$N_g(d)(x) = \sum_{v|d^\infty}\#\{p \leqslant x : p \equiv 1(\mathrm{mod}\ dv),\ v|r_p(g) \text{ and } (\frac{r_p(g)}{v}, d) = 1\}.$$

Let p be a prime counted on the right hand side. Note that it is counted only once, namely for $v = (r_p(g), d^\infty)$. From $\mathrm{ord}_p(g)r_p(g) = p-1$ it is then inferred that $d|\mathrm{ord}_p(g)$. Hence every prime counted on the right hand side is counted on the left hand side as well. Next consider a prime p counted by $N_g(d)(x)$. It satisfies $p \equiv 1(\mathrm{mod}\ d)$. Note there is a (unique) integer v such that $v|d^\infty$, $p \equiv 1(\mathrm{mod}\ dv)$ and $(r_p(g)/v, d) = 1$. Thus p is also counted on the right hand side. ∎

Remark 1. From (1) and Chebotarev's density theorem it follows that

$$0 \leqslant \sum_{\alpha|d}\frac{\mu(\alpha)}{[K_{dv,\alpha v}:\mathbb{Q}]} \leqslant \frac{1}{[K_{dv,v}:\mathbb{Q}]}. \quad (2)$$

3. Analytic consequences

Using Proposition 1 it is rather straightforward to establish that $N_g(d)$ has a natural density $\delta_g(d)$.

Lemma 1. *Write $g = g_1/g_2$ with g_1 and g_2 integers. Then*

$$N_g(d)(x) = \left(\delta_g(d) + O_{d,g}\left(\frac{(\log\log x)^{\omega(d)}}{\log^{1/8} x}\right)\right)\mathrm{Li}(x), \tag{3}$$

where the implied constant depends at most on d and g and

$$\delta_g(d) = \sum_{v|d^\infty}\sum_{\alpha|d}\frac{\mu(\alpha)}{[K_{dv,\alpha v}:\mathbb{Q}]}. \tag{4}$$

Corollary 1. *The set $N_g(d)$ has a natural density $\delta_g(d)$.*

The proof of Lemma 1 makes use of the following consequence of the Brun-Titchmarsh inequality.

Lemma 2. *Let $\pi(x;l,k) = \sum_{p\leqslant x,\ p\equiv l (\mathrm{mod}\ k)} 1$. Then*

$$\sum_{\substack{v>z\\ v|d^\infty}} \pi(x;dv,1) = O_d\left(\frac{x}{\log x}\frac{(\log z)^{\omega(d)}}{z}\right),$$

uniformly for $3 \leqslant z \leqslant \sqrt{x}$.

Proof. On noting that $M_d(x) := \#\{v \leqslant x : v|d^\infty\} \leqslant (\log x)^{\omega(d)}/\log 2$, it straightforwardly follows that

$$\sum_{\substack{v>z\\ v|d^\infty}}\frac{1}{v} = \int_z^\infty \frac{dM_d(z)}{z} \ll_d \frac{(\log z)^{\omega(d)}}{z}.$$

By the Brun-Titchmarsh inequality we have $\pi(x;w,1) \ll x/(\varphi(w)\log(x/w))$, where the implied constant is absolute and $w < x$. Thus

$$\sum_{\substack{z<v,\ dv\leqslant x^{2/3}\\ v|d^\infty}} \pi(x;dv,1) \ll \frac{x}{\varphi(d)\log x}\sum_{\substack{v>z\\ v|d^\infty}}\frac{1}{v} \ll_d \frac{x}{\log x}\frac{(\log z)^{\omega(d)}}{z}. \tag{5}$$

Using the trivial estimate $\pi(x;d,1) \leqslant x/d$ we see that

$$\sum_{\substack{dv>x^{2/3}\\ d|v^\infty}} \pi(x;dv,1) \leqslant \sum_{\substack{dv>x^{2/3}\\ v|d^\infty}}\frac{x}{dv} \leqslant \sum_{\substack{w>x^{2/3}\\ w|d^\infty}}\frac{x}{w} \ll_d x^{1/3}(\log x)^{\omega(d)}. \tag{6}$$

On combining (5) and (6) the proof is readily completed. ∎

Proof of Lemma 1. From [10, Lemma 2.1] we recall that there exist absolute constants A and B such that if $v \leqslant B(\log x)^{1/8}/d$, then

$$\pi_{K_{dv,\alpha v}}(x) = \frac{\mathrm{Li}(x)}{[K_{dv,\alpha v}:\mathbb{Q}]} + O_g(xe^{-\frac{A}{dv}\sqrt{\log x}}). \tag{7}$$

Let $y = B(\log x)^{1/8}/d$. From the proof of Proposition 1 we see that

$$N_g(d)(x) = \sum_{\substack{v|d^\infty \\ v\leqslant y}} \sum_{\alpha|d} \mu(\alpha)\pi_{K_{dv,\alpha v}}(x) + O\left(\sum_{\substack{v>y \\ v|d^\infty}} \pi(x;dv,1)\right) = I_1 + O(I_2),$$

say. By Lemma 2 we obtain that $I_2 = O(x(\log\log x)^{\omega(d)}\log^{-9/8} x)$. Now, by (7), we obtain

$$I_1 = \sum_{\substack{v|d^\infty \\ v\leqslant y}} \sum_{\alpha|d} \frac{\mu(\alpha)}{[K_{dv,\alpha v}:\mathbb{Q}]} + O_{d,g}(y\frac{x}{\log^{5/4} x}).$$

Denote the latter double sum by I_3. Keeping in mind Remark 1 we obtain

$$I_3 = \delta_g(d) + O\left(\sum_{\substack{v|d^\infty \\ v>y}} \sum_{\alpha|d} \frac{\mu(\alpha)}{[K_{dv,\alpha v}:\mathbb{Q}]}\right).$$

Using (2) and Lemma 3 it follows that

$$\sum_{\substack{v|d^\infty \\ v>y}} \sum_{\alpha|d} \frac{\mu(\alpha)}{[K_{dv,\alpha v}:\mathbb{Q}]} = O\left(\sum_{\substack{v|d^\infty \\ v>y}} \frac{1}{[K_{dv,v}:\mathbb{Q}]}\right) = O(\frac{1}{\varphi(d)}\sum_{\substack{v|d^\infty \\ v>y}} \frac{h}{v^2})$$
$$= O_d(\frac{h(\log y)^{\omega(d)}}{y}) = O_{d,g}\left(\frac{(\log y)^{\omega(d)}}{y}\right),$$

and hence

$$I_3 = \delta_g(d) + O_{d,g}\left(\frac{(\log y)^{\omega(d)}}{y}\right).$$

The result follows on collecting the various estimates. ∎

4. The evaluation of the density $\delta_g(d)$

A crucial ingredient in the evaluation of $\delta_g(d)$ is the following lemma.

Lemma 3. [6] *Write $g = \pm g_0^h$, where g_0 is positive and not an exact power of a rational. Let $D(g_0)$ denote the discriminant of the field $\mathbb{Q}(\sqrt{g_0})$. Put $m = D(g_0)/2$ if $\nu_2(h) = 0$ and $D(g_0) \equiv 4 (\mathrm{mod}\ 8)$ or $\nu_2(h) = 1$ and $D(g_0) \equiv 0 (\mathrm{mod}\ 8)$, and $m = [2^{\nu_2(h)+2}, D(g_0)]$ otherwise. Put*

$$n_r = \begin{cases} m & \text{if } g < 0 \text{ and } r \text{ is odd;} \\ [2^{\nu_2(hr)+1}, D(g_0)] & \text{otherwise.} \end{cases}$$

We have

$$[K_{kr,k} : \mathbb{Q}] = [\mathbb{Q}(\zeta_{kr}, g^{1/k}) : \mathbb{Q}] = \frac{\varphi(kr)k}{\epsilon(kr,k)(k,h)},$$

where, for $g > 0$ or $g < 0$ and r even we have

$$\epsilon(kr,k) = \begin{cases} 2 & \text{if } n_r | kr; \\ 1 & \text{if } n_r \nmid kr, \end{cases}$$

and for $g < 0$ and r odd we have

$$\epsilon(kr,k) = \begin{cases} 2 & \text{if } n_r | kr; \\ \frac{1}{2} & \text{if } 2|k \text{ and } 2^{\nu_2(h)+1} \nmid k; \\ 1 & \text{otherwise.} \end{cases}$$

Remark 2. Note that if h is odd, then $n_r = [2^{\nu_2(r)+1}, D(g)]$. Note that $n_r = n_{2^{\nu_2(r)}}$.

The 'generic' degree of $[K_{dv,\alpha v} : \mathbb{Q}]$ equals $\varphi(dv)\alpha v/(\alpha v, h)$ and on substituting this value in (4) we obtain the quantity S_1 which is evaluated in the following lemma.

Lemma 4. *We have*

$$S_1 := \sum_{v|d^\infty} \sum_{\alpha|d} \frac{\mu(\alpha)(\alpha v, h)}{\varphi(dv)\alpha v} = S(d,h),$$

where

$$S(d,h) := \frac{1}{d(h,d^\infty)} \prod_{p|d} \frac{p^2}{p^2-1}.$$

Proof. Since for $v|d^\infty$ we have $\varphi(dv) = v\varphi(d)$, we can write

$$S_1 = \frac{1}{\varphi(d)} \sum_{v|d^\infty} \sum_{\alpha|d} \frac{\mu(\alpha)(\alpha v, h)}{\alpha v^2} = \frac{1}{\varphi(d)} \sum_{v|d^\infty} \frac{(v,h)}{v^2} \sum_{\alpha|d} \frac{\mu(\alpha)(\alpha v, h)}{\alpha(v,h)}.$$

The expression in the inner sum is multiplicative in α and hence

$$\sum_{\alpha|d} \frac{\mu(\alpha)(\alpha v, h)}{\alpha(v,h)} = \prod_{p|d} \left(1 - \frac{(pv,h)}{p(v,h)}\right) = \begin{cases} \frac{\varphi(d)}{d} & \text{if } (h,d^\infty)|(v,d^\infty); \\ 0 & \text{otherwise.} \end{cases}$$

On noting that $(v,h)/v^2$ is multiplicative in v and that for $k \geqslant \nu_p(h)$

$$\sum_{r=k}^{\infty} \frac{(p^r,h)}{p^{2r}} = \frac{p^{\nu_p(h)+2-2k}}{p^2-1},$$

one concludes that

$$S_1 = \frac{1}{d} \sum_{\substack{v \mid d^\infty \\ (h,d^\infty) \mid v}} \frac{(v,h)}{v^2} = \frac{1}{d} \prod_{p \mid d} \sum_{r \geqslant \nu_p(h)} \frac{(p^r,h)}{p^{2r}} = \frac{1}{d} \prod_{p \mid d} \frac{p^{2-\nu_p(h)}}{p^2-1} = S(d,h).$$

This completes the proof. ∎

Remark 3. Note that the condition $(h,d^\infty) \mid (v,d^\infty)$ is equivalent with $\nu_p(v) \geqslant \nu_p(h)$ for all primes p dividing d.

By a minor modification of the proof of the latter result we infer:

Lemma 5. *Let $k \geqslant 0$ be an integer. Then*

$$S_2(k) := \sum_{\substack{v \mid d^\infty \\ \nu_2(v) \geqslant \nu_2(h)+k}} \sum_{\alpha \mid d} \frac{\mu(\alpha)(\alpha v,h)}{\varphi(dv)\alpha v} = 4^{-k} S(d,h).$$

The next lemma gives an evaluation of yet another variant of S_1.

Lemma 6. *Let D be a fundamental discriminant. Then*

$$S_3(D) := \sum_{\substack{v \mid d^\infty \\ [2^{\nu_2(hd/\alpha)+1}, D] \nmid dv}} \sum_{\alpha \mid d} \frac{\mu(\alpha)(\alpha v,h)}{\varphi(dv)\alpha v} = \begin{cases} 4^{-\gamma} S(d,h) & \text{if } 2 \mid d,\ D \mid 4d \text{ and } \gamma \geqslant 1; \\ -\frac{S(d,h)}{2} & \text{if } 2 \mid d,\ D \mid 4d \text{ and } \gamma = 0; \\ 0 & \text{otherwise,} \end{cases}$$

where $\gamma = \max\{0, \nu_2(D/dh)\}$.

Proof. The integer $[2^{\nu_2(hd/\alpha)+1}, D]$ is even and is required to divide d^∞, hence $S_3(D) = 0$ if d is odd. Assume that d is even. If D has an odd prime divisor not dividing d, then $D \nmid d^\infty$ and hence $S_3(D) = 0$. On noting that $\nu_2(D) \leqslant \nu_2(4d)$ and that the odd part of D is squarefree, it follows that if $S_3(D) \neq 0$, then $D \mid 4d$. So assume that $2 \mid d$ and $D \mid 4d$. Note that the condition $[2^{\nu_2(hd/\alpha)+1}, D] \mid dv$ is equivalent with $\nu_2(v) \geqslant \nu_2(h) + \max\{1, \nu_2(D/dh)\}$ for the α that are odd, and $\nu_2(v) \geqslant \nu_2(h) + \gamma$ for the even α. Thus if $\gamma \geqslant 1$ the condition $[2^{\nu_2(hd/\alpha)+1}, D] \mid dv$ is equivalent with $\nu_2(v) \geqslant \nu_2(h) + \gamma$ and then, by Lemma 5, $S_3(D) = S_2(\gamma) = 4^{-\gamma} S(d,h)$. If $\gamma = 0$ then

$$S_3(D) = S_2(0) - \sum_{\substack{v \mid d^\infty \\ \nu_2(v) = \nu_2(h)}} \sum_{\substack{\alpha \mid d \\ 2 \nmid \alpha}} \frac{\mu(\alpha)(\alpha v,h)}{\varphi(dv)\alpha v}.$$

By Lemma 5 it follows that $S_2(0) = S(d,h)$. A variation of Lemma 4 yields that the latter double sum equals $3S(d,h)/2$. ■

Remark 4. Put

$$\epsilon_2(D) = \begin{cases} (-1/2)^{2^{\max\{0,\nu_2(D/dh)\}}} & \text{if } 2|d \text{ and } D|4d; \\ 0 & \text{otherwise.} \end{cases}$$

Note that Lemma 6 can be rephrased as stating that if D is a fundamental discriminant, then $S_3(D) = \epsilon_2(D)S(d,h)$.

Let $g > 0$. It turns out that $\mathrm{ord}_p(g)$ is very closely related to $\mathrm{ord}_p(-g)$ and this can be used to express $N_{-g}(d)(x)$ in terms of $N_g(*)(x)$. From this $\delta_{-g}(d)$ is then easily evaluated, once one has evaluated $\delta_g(d)$.

Lemma 7. *Let $g > 0$. Then*

$$N_{-g}(d)(x) = \begin{cases} N_g(\frac{d}{2})(x) + N_g(2d)(x) - N_g(d)(x) + O(1) & \text{if } d \equiv 2 (\mathrm{mod}\ 4); \\ N_g(d)(x) + O(1) & \text{otherwise.} \end{cases}$$

In particular,

$$\delta_{-g}(d) = \begin{cases} \delta_g(\frac{d}{2}) + \delta_g(2d) - \delta_g(d) & \text{if } d \equiv 2 (\mathrm{mod}\ 4); \\ \delta_g(d) & \text{otherwise.} \end{cases}$$

The proof of this lemma is a consequence of Corollary 1 and the following observation.

Lemma 8. *Let p be odd and $g \neq 0$ be a rational number. Suppose that $\nu_p(g) = 0$. Then*

$$\mathrm{ord}_p(-g) = \begin{cases} 2\mathrm{ord}_p(g) & \text{if } 2 \nmid \mathrm{ord}_p(g); \\ \mathrm{ord}_p(g)/2 & \text{if } \mathrm{ord}_p(g) \equiv 2 (\mathrm{mod}\ 4); \\ \mathrm{ord}_p(g) & \text{if } 4|\mathrm{ord}_p(g). \end{cases}$$

Proof. Left to the reader. ■

Remark 5. It is of course also possible to evaluate $\delta_g(d)$ for negative g using the expression (4) and Lemma 3, however, this turns out to be rather more cumbersome than proceeding as above.

5. The proofs of Theorems 2 and 3

Proof of Theorem 2. By Lemma 1 it suffices to show that

$$\sum_{v|d^\infty} \sum_{\alpha|d} \frac{\mu(\alpha)}{[K_{dv,\alpha v} : \mathbb{Q}]} = \epsilon_1 S(d,h)$$

If $g > 0$, then it follows by Lemma 3 that $\delta_g(d) = S_1 + S_3(D(g_0))$ and by Lemmas 4 and 6 (with $D = D(g_0)$), the claimed evaluation then results in this case. If h

is odd, then similarly, $\delta_g(d) = S_1 + S_3(D(g))$ (cf. the remark following Lemma 3) and, again by Lemma 4 and 6, the claimed evaluation then is deduced in this case. If $g < 0$, the result follows after some computation on invoking Lemma 7 and the result for $g > 0$. ∎

Proof of Theorem 3. Recall that $\pi_L(x)$ denotes the number of unramified primes $p \leqslant x$ that split completely in the number field L. Under GRH it is known, cf. [5], that

$$\pi_L(x) = \frac{\mathrm{Li}(x)}{[L:\mathbb{Q}]} + O\left(\frac{\sqrt{x}}{[L:\mathbb{Q}]}\log(d_L x^{[L:\mathbb{Q}]})\right),$$

where d_L denotes the absolute discriminant of L. From this it follows on using the estimate $\log|d_{K_{dv_1,\alpha v}}| \leqslant dv(\log(dv) + \log|g_1 g_2|)$ from [6] that, uniformly in v,

$$\pi_{K_{dv,\alpha v}}(x) = \frac{\mathrm{Li}(x)}{[K_{dv,\alpha v}:\mathbb{Q}]} + O_{d,g}(\sqrt{x}\log x),$$

where α is an arbitrary divisor of d. On noting that in Proposition 1 we can restrict to those integers v satisfying $dv \leqslant x$ and hence the number of non-zero terms in Proposition 1 is bounded above by $2^{\omega(d)}(\log x)^{\omega(d)}$, the result easily follows. ∎

6. Some examples

In this section we provide some numerical demonstration of our results.

The numbers in the column 'experimental' arose on counting how many primes $p \leqslant p_{10^8} = 2038074743$ with $\nu_p(g) = 0$, satisfy $d|\mathrm{ord}_p(g)$.

Table 2: The case $g > 0$

g	g_0	h	$D(g_0)$	d	ϵ_1	$\delta_g(d)$	numerical	experimental
2	2	1	8	2	17/16	17/24	$0.70833333\cdots$	0.70831919
2	2	1	8	4	5/4	5/12	$0.41666666\cdots$	0.41667021
2	2	1	8	8	1/2	1/12	$0.08333333\cdots$	0.08333144
3	3	1	12	11	1	11/120	$0.09166666\cdots$	0.09165950
3	3	1	12	12	1/2	1/16	$0.06250000\cdots$	0.06249098
4	2	2	8	5	1	5/24	$0.20833333\cdots$	0.20833328
4	2	2	8	6	5/4	5/32	$0.15625000\cdots$	0.15625824

Table 3: The case $g < 0$

g	g_0	h	$D(g_0)$	d	ϵ_1	$\delta_g(d)$	numerical	experimental
-2	2	1	8	2	17/16	17/24	$0.70833333\cdots$	0.70835101
-2	2	1	8	4	5/4	5/12	$0.41666666\cdots$	0.41667021
-2	2	1	8	6	17/16	17/64	$0.26562500\cdots$	0.26562628
-3	3	1	12	5	1	5/24	$0.20833333\cdots$	0.20834107
-3	3	1	12	12	1/2	1/16	$0.06250000\cdots$	0.06249098
-4	2	2	8	2	2	2/3	$0.66666666\cdots$	0.66666122
-4	2	2	8	4	1/2	1/8	$0.08333333\cdots$	0.08333144
-9	3	2	12	2	5/2	5/6	$0.83333333\cdots$	0.83333215
-9	3	2	12	6	11/4	11/32	$0.34375000\cdots$	0.34375638

Acknowledgement. I like to thank Francesco Pappalardi for sending me his paper [10]. Theorem 1.3 in that paper made me realize that a relatively simple formula for $\delta_g(d)$ exists. The data in the tables are produced by a C^{++} program kindly written by Yves Gallot.

References

[1] C. Ballot, *Density of prime divisors of linear recurrences*, Mem. Amer. Math. Soc. **115** (1995), no. 551, viii+102 pp.

[2] K. Chinen and L. Murata, *On a distribution property of the residual order of* $a(\text{mod } p)$. I, J. Number Theory **105** (2004), 60–81.

[3] H. Hasse, *Über die Dichte der Primzahlen p, für die eine vorgegebene ganzrationale Zahl a* $\neq 0$ *von durch eine vorgegebene Primzahl* $l \neq 2$ *teilbarer bzw. unteilbarer Ordnung* mod. p *ist*, Math. Ann. **162** (1965/1966), 74–76.

[4] H. Hasse, *Über die Dichte der Primzahlen p, für die eine vorgegebene ganzrationale Zahl a* $\neq 0$ *von gerader bzw.ungerader Ordnung mod. p ist*, Math. Ann. **166** (1966), 19–23.

[5] S. Lang, *On the zeta function of number fields*, Invent. Math. **12** (1971), 337–345.

[6] P. Moree, *On the distribution of the order and index of* $g(\text{mod } p)$ *over residue classes I, arXiv:math.*NT/0211259, J. Number Theory, to appear.

[7] P. Moree, *Asymptotically exact heuristics for prime divisors of the sequence* $\{a^k + b^k\}_{k=1}^{\infty}$, *arXiv:math.*NT/0311483, submitted (already electronically available).

[8] L. Murata and K. Chinen, *On a distribution property of the residual order of* $a(\text{mod } p)$. II, J. Number Theory **105** (2004), 82–100.

[9] R.W.K. Odoni, *A conjecture of Krishnamurthy on decimal periods and some allied problems*, J. Number Theory **13** (1981), 303–319.
[10] F. Pappalardi, *Square free values of the order function*, New York J. Math. **9** (2003), 331-344.
[11] K. Wiertelak, *On the density of some sets of primes*. I, Acta Arith. **34** (1977/78), 183–196.
[12] K. Wiertelak, *On the density of some sets of primes*. II, Acta Arith. **34** (1977/78), 197–210.
[13] K. Wiertelak, *On the density of some sets of primes*. III, Funct. Approx. Comment. Math. **10** (1981), 93–103.
[14] K. Wiertelak, *On the density of some sets of primes*. III. Studies in pure mathematics, 761–773, Birkhäuser, Basel, 1983.
[15] K. Wiertelak, *On the density of some sets of primes*. IV, Acta Arith. **43** (1984), 177–190.
[16] K. Wiertelak, *On the density of some sets of integers*, Funct. Approx. Comment. Math. **19** (1990), 71–76.
[17] K. Wiertelak, *On the density of some sets of primes p, for which* $(\mathrm{ord}_p\, b, n) = d$, Funct. Approx. Comment. Math. **21** (1992), 69–73.
[18] K. Wiertelak, *On the distribution of the smallest natural numbers having order mod p not coprime with a given integer*, Acta Math. Hungar. **80** (1998), 271–284.
[19] K. Wiertelak, *On the density of some sets of primes p, for which* $n|\mathrm{ord}_p a$, Funct. Approx. Comment. Math. **28** (2000), 237–241.

Address: Pieter Moree, Max-Planck-Institut für Mathematik, Vivatsgasse 7, D-53111 Bonn, Germany.
E-mail: moree@mpim-bonn.mpg.de
Received: 27 July 2004