SQUARE FREE VALUES OF THE ORDER FUNCTION

FRANCESCO PAPPALARDI

Abstract. Given $a \in \mathbb{Z} \setminus \{\pm 1, 0\}$, we consider the problem of enumerating the integers m coprime to a such that the order of a modulo m is square free. This question is raised in analogy to a result recently proved jointly with F. Saidak and I. Shparlinski where square free values of the Carmichael function are studied. The technique is the one of Hooley that uses the Chebotarev Density Theorem to enumerate primes for which the index $i_p(a)$ of a modulo p is divisible by a given integer.

1. Introduction

The goal of this paper is to study the following function:

$$I_a(x) = \#\{m \le x \mid (m,a) = 1,\, l_m(a) \,\text{is square free}\}$$

where $a \in \mathbb{Z} \setminus \{\pm 1, 0\}$, and $l_m(a)$ denotes the multiplicative order of a in $(\mathbb{Z}/m\mathbb{Z})^*$. This question is somehow analogue to the question treated in [10] where it is determined an asymptotic formula for the number of integers up to x for which the value of the Carmichael function is square free.

We will prove the following:

Theorem 1.1. *Given $a \in \mathbb{Z} \setminus \{\pm 1, 0\}$, there exist constants α_a and β_a (defined in (1)) such that:*

$$I_a(x) = (\alpha_a + o(1))\, x \log^{\beta_a - 1} x.$$

If $a \in \mathbb{Z} \setminus \{\pm 1, 0\}$, we write $a = b^h$ with b not a power of any integer and $b = a_1 a_2^2$ with a_1 square free.

We will deduce Theorem 1.1 from the following:

Theorem 1.2. *Let $\mathrm{Li}(x) = \int_0^x \frac{dt}{\log t}$ denote the logarithmic integral function. With the above notations we have that*

$$J_a(x) = \#\{p \le x \mid p \nmid a,\ l_p(a) \text{ is square free}\} = \left(\beta_a + O\left(\frac{1}{\log^{1/25} x}\right)\right) \mathrm{Li}(x).$$

where if $v_l(h)$ denotes the l–adic valuation of h, then

$$(1)\quad \beta_a = \left[\prod_l \left(1 - \frac{1}{l^{v_l(h)}(l^2-1)}\right)\right] \cdot \left[1 + \left(\frac{-1}{2}\right)^{\frac{(2,a_1)}{(a_1,2,h)}} \prod_{l \mid [2,a_1]} \frac{1}{1 - l^{v_l(h)}(l^2-1)}\right].$$

1991 *Mathematics Subject Classification.* 11N37, 11N56.

Key words and phrases. Square free integers, Carmichael function, Wirsing theorem, Chebotarev density theorem.

Note that β_a is always a rational multiple of

$$\prod_l \left(1-\frac{1}{l^2-1}\right) = 0.53071189\cdots$$

and in the case when a is square free, the formula simplifies in

$$\beta_a = \left[1+\frac{1}{4}\prod_{l|a}\frac{1}{2-l^2}\right]\prod_l\left(1-\frac{1}{l^2-1}\right).$$

The main ingredient for the proof of Theorem 1.2 is the following result that has its own interest. Special cases of it also appeared in K. Chinen and L. Murata [2] ($m=4$) and in P. Moree [7] ($m=3,4$). In both papers the more difficult cases of non zero congruence classes are also considered. The statement in the case when m is prime, is a direct consequence of the work due to R. W. K. Odoni [8]. The result also appears in Wiertelak [11] with a weaker range of uniformity.

Theorem 1.3. *Let $m\in\mathbb{N}$, $a\in\mathbb{N}\setminus\{0,1\}$. Consider the function*

$$A_a(x,m) = \#\left\{p\le x\,|p\nmid a,\ m\mid l_p(a)\right\}.$$

Then, for every $\epsilon>0$, the following asymptotic formula holds uniformly on m:

$$A_a(x,m) = \left(\varsigma_{a,m}+O_a\left(\frac{m^{1-2\epsilon}}{\log^{1/8-\epsilon}x}\right)\right)\mathrm{Li}(x).$$

If $v_l(h)$ is the l–adic valuation of h and $(h,m^\infty)=\prod_{l|m}l^{v_l(h)}$, then

$$\varsigma_{a,m} = \frac{\nu_{a,m}}{m(h,m^\infty)}\prod_{l|m}\left(\frac{l^2}{l^2-1}\right)$$

where

$$\nu_{a,m} = \begin{cases} 1, & \text{if } [2,a_1]\nmid m;\\ 1/2, & \text{if } [2,a_1]\mid m, a_1\equiv 1 \bmod 4;\\ 1/2, & \text{if } [2,a_1]\mid m, a_1\not\equiv 1 \bmod 4, 4(2,a_1)\mid mh;\\ 5/4, & \text{if } [2,a_1]\mid m, a_1\not\equiv 1 \bmod 4, 2(2,a_1)\| mh;\\ 17/16, & \text{if } [2,a_1]\mid m, a_1\not\equiv 1 \bmod 4, 2(2,a_1)\nmid mh.\end{cases}$$

2. Lemmata from the literature

Let n and d be positive integers with $d\mid n$ and $a\in\mathbb{N}\setminus\{0,1\}$. We set

$$K_{n,d}=\mathbb{Q}(\zeta_n,a^{1/d}) \quad\text{and}\quad k_{n,d}=[K_{n,d}:\mathbb{Q}]=d'\varphi(n)/\vartheta \tag{2}$$

where $d'=d/(d,h)$, then

$$\vartheta=\vartheta(n,d)=\begin{cases}2, & \text{if } 2\mid d', a_1\mid n, \text{ and } a_1\equiv 1 \bmod 4,\\ 2, & \text{if } 2\mid d', 4a_1\mid n, \text{ and } a_1\not\equiv 1 \bmod 4,\\ 1, & \text{otherwise.}\end{cases} \tag{3}$$

The proof of formulas (2) and (3) can be found in many places. See for example [3, Lemma 2.2]. Since it will be needed later, we observe that $k_{n,d}$ is multiplicative in the following sense

$$k_{n_1,d_1}k_{n_2,d_2}=k_{n_1n_2,d_1d_2} \quad\text{when}\quad (n_1,n_2)=1 \text{ and } d_1\mid n_1, d_2\mid n_2. \tag{4}$$

Furthermore $\vartheta(l^\alpha,d)=1$ when $l>2$.

It is a criterion due to Dedekind that an odd prime p splits completely in $K_{n,d}$ if and only d divides the index $i_p(a) = (p-1)/l_p(a)$ of a modulo p and $p \equiv 1(\bmod n)$. Therefore we set $\pi(x, n, d)$ to be the number of primes up to x that are unramified and split completely in $K_{n,d}$ or equivalently

$$\pi(x,n,d) = \#\{p \le x \mid p \nmid a,\ p \equiv 1(\bmod n),\ d \mid i_p(a)\}. \tag{5}$$

Note that when $d = 1$, $\pi(x, n, 1)$ is the number of primes up to x not dividing a that are congruent to 1 modulo n.

The Chebotarev Density Theorem provides us with an asymptotic formula for $\pi(x, n, d)$. This was the main ingredient in the famous proof of Artin Conjecture subject to the Riemann Hypothesis due to C. Hooley [4]. The following result is due to Lagarias and Odlyzko [6]. Here we state the version that was used in [9, page 376]:

Lemma 2.1 (Chebotarev Density Theorem.)**.** *With the above notations, there exist absolute constants A and B such that if $n \le B(\log x)^{1/8}$, then*

$$\pi(x,n,d) = \frac{1}{k_{n,d}}\,\mathrm{Li}(x) + O\left(x\exp(-A\sqrt{\log x}/n)\right). \quad \square$$

We will also need the Theorem of Wirsing [12] that can be formulated as follows:

Lemma 2.2. *Assume that a real–valued multiplicative function $f(n)$ satisfies the following conditions:*

a. *$f(n) \ge 0$, $n = 1, 2, \ldots$;*
b. *$f(p^\nu) \le c_1 c_2^\nu$, $\nu = 2, 3, \ldots$, for some constants c_1, c_2 with $c_2 < 2$;*
c. *there exists a constant $\tau > 0$ such that*

$$\sum_{p\le x} f(p) = (\tau + o(1))\,\mathrm{Li}(x).$$

Then for any $x \ge 0$,

$$\sum_{n\le x} f(n) = \left(\frac{1}{e^{\gamma\tau}\Gamma(\tau)} + o(1)\right)\frac{x}{\log x}\prod_{p\le x}\sum_{\nu=0}^{\infty}\frac{f(p^\nu)}{p^\nu},$$

where γ is the Euler constant, and $\Gamma(s) = \int_0^\infty e^{-t}t^{s-1}\,dt$ is the gamma–function. $\square$

3. Divisibility of the order by an integer: proof of Theorem 1.3

The proof of Theorem 1.3 is based on the following Lemma.

Lemma 3.1. *Let $m \in \mathbb{Z}$, $a \in \mathbb{Z}\setminus\{\pm 1, 0\}$. With the notation of Theorem 1.3 and considering (5), we have that*

$$A_a(x,m) = \sum_{n\in\mathcal{S}_m}\sum_{d\mid m}\sum_{f\mid n}\mu(d)\mu(f)\pi(x, nd, \gamma(f, n/m))$$

where $m^0 = \prod_{l\mid m} l$ is the radical of m, $\mathcal{S}_m = \{n \in \mathbb{N}$ such that $n^0 \mid m$ and $m \mid n\}$ and

$$\gamma(f,k) = \prod_{l\mid f} l^{v_l(k)+1}.$$

Proof. Let p be a prime such that $p \nmid a$ and $m \mid l_p(a)$. Then $m \mid p-1$ and there exists a unique $n \in \mathcal{S}_m$ such that $p \equiv 1 \bmod n$ and $(\frac{p-1}{n}, m) = 1$ (indeed $n = \prod_{l|m} l^{v_l(p-1)}$).

Hence we can write

$$A_a(x,m) = \sum_{n\in\mathcal{S}_m} \#\left\{ p \le x \,\middle|\, p \nmid a,\ m \mid l_p(a),\ p \equiv 1(\operatorname{mod} n),\ (\frac{p-1}{n}, m) = 1 \right\}. \tag{6}$$

Now note that if p is a prime with $p \nmid a$, $p \equiv 1 \bmod n$ and $(\frac{p-1}{n}, m) = 1$, then

$$m \mid l_p(a) \quad\Longleftrightarrow\quad (i_p(a), n) \,\Big|\, \frac{n}{m}$$

where $i_p(a) = \frac{p-1}{l_p(a)}$ is the index of a modulo p. Indeed from the hypothesis that $n \in \mathcal{S}_m$ and from $n = (p-1, n) = (i_p(a), n)(l_p(a), n)$ we have that $m \mid l_p(a)$ if and only if $m \mid (l_p(a), n)$ i.e. $(i_p(a), n) \mid \frac{n}{m}$. So we can rewrite (6) as

$$A_a(x,m) = \sum_{n\in\mathcal{S}_m} \#\left\{ p \le x \,\middle|\, p \nmid a, (i_p(a), n) \,\Big|\, \frac{n}{m},\ p \equiv 1(\operatorname{mod} n), (\frac{p-1}{n}, m) = 1 \right\}. \tag{7}$$

Next we apply twice the inclusion exclusion formula; first to the conditions $p \equiv 1(\operatorname{mod} n), (\frac{p-1}{n}, m) = 1$, so that (7) equals

$$A_a(x,m) = \sum_{n\in\mathcal{S}_m} \sum_{d|m} \mu(d) \# \left\{ p \le x \,\middle|\, p \nmid a, (i_p(a), n) \,\Big|\, \frac{n}{m}\ , p \equiv 1(\operatorname{mod} nd) \right\} \tag{8}$$

and then to the condition $(i_p(a), n) \,\big|\, \frac{n}{m}$. So that (8) equals

$$A_a(x,m) = \sum_{n\in\mathcal{S}_m} \sum_{\substack{d|m \\ f|n}} \mu(d)\mu(f) \# \left\{ p \le x \,\middle|\, p \nmid a, \gamma(f, \frac{n}{m}) \mid i_p(a),\ p \equiv 1(\operatorname{mod} nd) \right\} \tag{9}$$

where $\gamma(f, n/m)$ is defined in the statement of the Lemma. Finally, using the definition in (5), we obtain the claim. $\square$

We will also need the following technical result:

Lemma 3.2. *With the notations above, let*

$$\varsigma_{a,m} = \sum_{n\in\mathcal{S}_m} \sum_{\substack{d|m \\ f|n}} \frac{\mu(d)\mu(f)}{k_{nd,\gamma(f,\frac{n}{m})}}.$$

Then

$$\varsigma_{a,m} = \frac{\nu_{a,m}}{m(m^\infty, h)} \prod_{l|m} \left(\frac{l^2}{l^2-1} \right)$$

where $\nu_{a,m}$ has been defined in the statement of Theorem 1.3.

Proof. We use the formulas for the degrees $k_{nd,\gamma(f,\frac{n}{m})}$ stated in (2) and (3):

$$k_{nd,\gamma(f,\frac{n}{m})} = d\varphi(n) \prod_{l|f} l^{\max(0, v_l(n/mh)+1)} \vartheta(nd, \gamma(f, \frac{n}{m})).$$

Write $\vartheta(nd, \gamma(f, \frac{n}{m})) = 1 + \psi$, where

$$\psi = \psi(f, m, n, d) = \begin{cases} 1, & \text{if } a_1 \equiv 1 \bmod 4,\ a_1|nd \text{ and } 2|\gamma(f, \frac{n}{m})'; \\ 1, & \text{if } a_1 \not\equiv 1 \bmod 4,\ 4a_1|nd \text{ and } 2|\gamma(f, \frac{n}{m})'; \\ 0, & \text{otherwise.} \end{cases}$$

For $\psi(f, m, n, d)$ to be non-zero, one must have $[2, a_1] \mid m$, $2 \mid f$ and $v_2(n/m) \geq v_2(h)$. In the second case, one must have additionally that $v_2(dn) \geq v_2(4a_1)$.

Thus our sum is

$$\sum_{n\in\mathcal{S}_m} \frac{1}{\varphi(n)} \sum_{d|m} \frac{\mu(d)}{d} \sum_{f|m} \frac{\mu(f)}{\prod_{l|f} l^{\max(0, v_l(n/mh)+1)}} (1 + \psi(f, m, n, d)) = \tag{10}$$

$$\sum_{n\in\mathcal{S}_m} \frac{\varphi(m)}{m\varphi(n)} \sum_{f|m} \frac{\mu(f)}{\prod_{l|f} l^{\max(0, v_l(\frac{n}{mh})+1)}} +$$

$$\sum_{n\in\mathcal{S}_m} \frac{1}{\varphi(n)} \sum_{d|m} \frac{\mu(d)}{d} \sum_{f|m} \frac{\mu(f)\psi(f, m, n, d)}{\prod_{l|f} l^{\max(0, v_l(\frac{n}{mh})+1)}}$$

By the multiplicative property of (4) and since $\varphi(n) = n\varphi(m)/m$, we deduce that the first sum above equals

$$\sum_{n\in\mathcal{S}_m} \frac{1}{n} \prod_{l|m} \left(1 - \frac{1}{l^{\max(0, v_l(n/mh)+1)}}\right)$$

$$= \prod_{l|m} \sum_{j\geq v_l(m)} \frac{1}{l^j} \left(1 - \frac{1}{l^{\max(0, j+1-v_l(mh))}}\right)$$

$$= \prod_{l|m} \sum_{j\geq v_l(mh)} \frac{1}{l^j} \left(1 - \frac{1}{l^{\max(0, j+1-v_l(mh))}}\right)$$

$$= \frac{1}{m(m^\infty, h)} \prod_{l|m} \sum_{j\geq 0} \frac{1}{l^j} \left(1 - \frac{1}{l^{j+1}}\right)$$

$$= \frac{1}{m(m^\infty, h)} \prod_{l|m} \frac{l^2}{l^2 - 1}. \tag{11}$$

The second sum in (10) only occurs when $[2, a_1]|m$, and then it equals

$$\sum_{\substack{n\in\mathcal{S}_m, \\ v_2(n/m)\geq v_2(h)}} \frac{1}{\varphi(n)} \sum_{\substack{d|m, \\ a_1\not\equiv 1 \bmod 4 \ \Rightarrow \ v_2(dn)\geq v_2(4a_1)}} \frac{\mu(d)}{d} \sum_{f|m, 2|f} \frac{\mu(f)}{\prod_{l|f} l^{\max(0, v_l(n/mh)+1)}}$$

Each summand is the same multiplicative function as in the first sum. The difference here is the range in the sum for the 2-part. Thus the l-part of the sums are the same for each $l > 2$. Taking $V = v_2(mh)$, the 2–part in (11) is $\frac{4}{3\cdot 2^V}$; the 2–part here is

$$2 \sum_{j\geq V} \frac{1}{2^j} \left(1 - \frac{1}{2}\right) \frac{-1}{2^{j-V+1}} = -\frac{2}{3 \cdot 2^V}$$

if $a_1 \equiv 1 (\mathrm{mod} 4)$ and it is

$$2 \sum_{j\geq V} \frac{1}{2^j} \cdot S_j \cdot \frac{-1}{2^{j-V+1}}$$

if $a_1 \not\equiv 1(\mathrm{mod} 4)$, where the S_j (the intermediate sum) is

$$S_j = \sum_{\substack{d|m,\\ j+v_2(d)\geq v_2(4a_1)}} \frac{\mu(d)}{d} = \begin{cases} 0, & \text{if } j \leq v_2(a_1); \\ -\frac{1}{2}, & \text{if } j = v_2(a_1)+1; \\ \frac{1}{2}, & \text{if } j \geq v_2(4a_1). \end{cases}$$

Now since $V \geq v_2(a_1)$ when $a_1 \not\equiv 1(\mathrm{mod} 4)$, the 2-part equals

$$2\sum_{j\geq V} \frac{1}{2^j} \cdot S_j \cdot \frac{-1}{2^{j-V+1}} = \begin{cases} \frac{1}{3\cdot 2^{V+2}}, & \text{if } V = v_2(a_1); \\ \frac{1}{3\cdot 2^{V}}, & \text{if } V = v_2(a_1)+1; \\ -\frac{1}{3\cdot 2^{V-1}}, & \text{if } V \geq v_2(4a_1). \end{cases}$$

Finally in all cases we deduce

$$\varsigma_{a,m} = \frac{1}{m(m^\infty,h)} \prod_{l|m} \frac{l^2}{l^2-1} \cdot \begin{cases} 1, & \text{if } [2,a_1] \nmid m; \\ 1/2, & \text{if } [2,a_1] \mid m \text{ and } a_1 \equiv 1 \bmod 4; \\ 17/16, & \text{if } [2,a_1] \mid m \text{ and } a_1 \not\equiv 1 \bmod 4, 2 \nmid \frac{hm}{(a_1,hm)}; \\ 5/4, & \text{if } [2,a_1] \mid m \text{ and } a_1 \not\equiv 1 \bmod 4, 2 \| \frac{hm}{(a_1,hm)}; \\ 1/2, & \text{if } [2,a_1] \mid m \text{ and } a_1 \not\equiv 1 \bmod 4, 4 \mid \frac{hm}{(a_1,hm)}. \end{cases}$$

□

Lemma 3.3. *Let $\mathcal{S}_m = \{n \in \mathbb{N} \mid n^0 \mid m \mid n\}$ be as in the statement of Lemma 3.1. Then, for any $c \in (0,1)$, uniformly on m,*

$$\sum_{\substack{n\in\mathcal{S}_m\\ n\geq T}} \frac{1}{n} \ll_c \frac{1}{T^c}.$$

Proof. This is an application of the Rankin method. For any $0 < c < 1$ we have

$$\begin{aligned} \sum_{\substack{n\in\mathcal{S}_m\\ n\geq T}} \frac{1}{n} &\leq \sum_{n\in\mathcal{S}_m} \frac{1}{n}\cdot\left(\frac{n}{T}\right)^c = \frac{1}{T^c}\sum_{n\in\mathcal{S}_m}\frac{1}{n^{1-c}} \\ &= \frac{1}{T^c m^{1-c}} \sum_{\substack{r\geq 1,\\ p|r \Rightarrow p|m}} \frac{1}{r^{1-c}} = \frac{1}{T^c m^{1-c}} \prod_{p|m}\left(1-\frac{1}{p^{1-c}}\right)^{-1} \\ &\leq \frac{1}{T^c}\prod_{p|m}\frac{1}{p^{1-c}-1} \ll_c \frac{1}{T^c}. \end{aligned}$$

□

Proof of Theorem 1.3. Let us start from the identity of Lemma 3.1 and rewrite it as:

$$\begin{aligned}
A_a(x,m) &= \sum_{\substack{n\in\mathcal{S}_m,\\ nm\le y}}\sum_{\substack{d\mid m\\ f\mid n}}\mu(d)\mu(f)\pi\left(x,nd,\gamma\left(f,\frac{n}{m}\right)\right)+\\
&\quad O\left(\sum_{\substack{n\in\mathcal{S}_m,\\ nm>y}}\sum_{\substack{d\mid m\\ f\mid n}}\pi\left(x,nd,\gamma\left(f,\frac{n}{m}\right)\right)\right)\\
&= \Sigma_1+O(\Sigma_2).
\end{aligned}$$

Note that Lemma 2.1 implies that if $y=B\log x^{1/8}$, then

$$\begin{aligned}
\Sigma_1 &= \sum_{\substack{n\in\mathcal{S}_m,\\ nm\le y}}\sum_{\substack{d\mid m\\ f\mid n}}\mu(d)\mu(f)\pi\left(x,nd,\gamma\left(f,\frac{n}{m}\right)\right)\\
&= \sum_{\substack{n\in\mathcal{S}_m,\\ nm\le y}}\sum_{\substack{d\mid m\\ f\mid n}}\left(\frac{\mu(d)\mu(f)\operatorname{Li}(x)}{k_{dn,\gamma(f,\frac{n}{m})}}+O\left(x\exp -A\frac{\sqrt{\log x}}{nm}\right)\right)\\
&= \varsigma_{m,a}\operatorname{Li}(x)+E(x,y,m),
\end{aligned}$$

where

$$\begin{aligned}
E(x,y,m) &\ll \sum_{\substack{n\in\mathcal{S}_m,\\ nm\le y}}\frac{\tau(n)\tau(m)x}{\exp\left(A\frac{\sqrt{\log x}}{nm}\right)}+\sum_{\substack{n\in\mathcal{S}_m,\\ nm>y}}\sum_{\substack{d\mid m\\ f\mid n}}\frac{\mu(d)\mu(f)}{k_{dn,\gamma(f,n/m)}}\operatorname{Li}(x)\\
&\ll \frac{\tau(m)}{m}\frac{xy\log y}{\exp\left(A\frac{\sqrt{\log x}}{y}\right)}+\frac{\tau(m)m}{\varphi(m)}\frac{x}{\log x}\sum_{\substack{n\in\mathcal{S}_m,\\ n>y/m}}\frac{1}{\varphi(n)},
\end{aligned}$$

since $k_{dn,\gamma(f,n/m)}\gg d\varphi(n)$. The fact that $m\le y$ implies that the first term is negligible. For the second term observe that, from Lemma 3.3, we have for any $0<c<1$:

$$\begin{aligned}
\frac{\tau(m)m}{\varphi(m)}\frac{x}{\log x}\sum_{\substack{n\in\mathcal{S}_m,\\ n>y/m}}\frac{1}{\varphi(n)} &= \frac{\tau(m)m^2}{\varphi(m)^2}\frac{x}{\log x}\sum_{\substack{n\in\mathcal{S}_m,\\ n>y/m}}\frac{1}{n}\\
&\le \frac{\tau(m)m^2}{\varphi(m)^2}\frac{x}{\log x}\frac{m^c}{y^c}\ll m^{c+\epsilon}\frac{x}{(\log x)^{1+c/8}}.
\end{aligned}$$

Now let us deal with Σ_2. We have that

$$\sum_{\substack{n\in\mathcal{S}_m,\\ nm>y}}\sum_{\substack{d\mid m\\ f\mid n}}\pi\left(x,nd,\gamma\left(f,\frac{n}{m}\right)\right)\ll$$

$$\tau(m)\left(\sum_{\substack{n\in\mathcal{S}_m,\\ y<nm\le z}}\sum_{d\mid m}\pi\left(x,nd,1\right)+\sum_{\substack{n\in\mathcal{S}_m,\\ nm>z}}\sum_{d\mid m}\#\{k\le x\mid nd\mid k\}\right),$$

where z is a suitable parameter that will be determined momentarily. By the Brun–Tichmarch Theorem and the trivial estimate, the above is

$$\ll \frac{\tau(m)m}{\varphi(m)}x\left(\frac{1}{\log(x/z)}\sum_{\substack{n\in\mathcal{S}_m,\\ nm>y}}\frac{1}{\varphi(n)}+\sum_{\substack{n\in\mathcal{S}_m,\\ nm>z}}\frac{1}{n}\right).$$

Finally setting $z=\log^{2+1/c}x$, say, and applying Lemma 3.3 as before, we obtain the claim. □

4. Square free orders modulo primes: proof of Theorem 1.2

Let us start by noticing that since

$$l_p(-a)=\begin{cases}2l_p(a), & \text{if } l_p(a) \text{ is odd;}\\ l_p(a), & \text{if } l_p(a) \text{ and } l_p(-a) \text{ are both even;}\\ l_p(a)/2, & \text{if } l_p(a) \text{ is even and } l_p(-a) \text{ is odd,}\end{cases}$$

$l_p(a)$ is square free if and only if $l_p(-a)$ is square free. Therefore we can assume $a\in\mathbb{N}$ and apply Theorem 1.3.

From the standard formula $\mu(k)^2=\sum_{d^2|k}\mu(d)$ we deduce that

$$J_a(x)=\#\{p\le x\mid p\nmid a, l_p(a) \text{ is square free}\}=\sum_{p\le x, p\nmid a}\mu(l_p(a))^2=$$

$$=\sum_{m=1}^{\infty}\mu(m)A_a(x,m^2)=\sum_{m\le\log^{1/25}x}\mu(m)A_a(x,m^2)+\sum_{m>\log^{1/25}x}\mu(m)A_a(x,m^2)=$$

$$\sum_{m=1}^{\infty}\mu(m)\varsigma_{a,m^2}\operatorname{Li}(x)+ \tag{12}$$

$$+O\left(\sum_{m\le\log^{1/25}x}\frac{xm^{1-2\epsilon}}{\log^{9/8-\epsilon}x}+\sum_{m>\log^{1/25}x}\left(\varsigma_{a,m^2}\operatorname{Li}(x)+A_a(x,m^2)\right)\right).$$

Also note that from Theorem 1.3, if m is square free,

$$\varsigma_{a,m^2}=\frac{\varepsilon}{(m^\infty,h)}\prod_{l|m}\frac{1}{l^2-1}\quad\text{where } \varepsilon=\begin{cases}1, & \text{if } [2,a_1]\nmid m;\\ 1+\left(\frac{-1}{2}\right)^{\frac{(a_1,2)}{(a_1,2,h)}}, & \text{if } [2,a_1]\mid m.\end{cases}$$

Therefore

$$\sum_{m=1}^{\infty}\mu(m)\varsigma_{a,m^2}=\sum_{[2,a_1]\nmid m}\mu(m)\varsigma_{a,m^2}+\sum_{[2,a_1]|m}\mu(m)\varsigma_{a,m^2}\quad=$$

$$\sum_{m=1}^{\infty}\frac{\mu(m)}{(m^\infty,h)}\prod_{l|m}\frac{1}{l^2-1}+\left(\frac{-1}{2}\right)^{(a_1,2)/(a_1,2,h)}\sum_{\substack{m=1\\ [2,a_1]|m}}^{\infty}\frac{\mu(m)}{(m^\infty,h)}\prod_{l|m}\frac{1}{l^2-1}\quad=$$

$$\prod_{l}\left(1-\frac{1}{l^{v_h(l)}(l^2-1)}\right)\left(1+\left(\frac{-1}{2}\right)^{\frac{(a_1,2)}{(a_1,2,h)}}\mu([2,a_1])\prod_{l|[2,a_1]}\frac{1}{l^{v_l(h)}(l-1)-1}\right)$$

which is the formula in the statement.

It remains to estimate the error term in (12). The first sum is

$$\ll \sum_{m\le \log^{1/25} x} \frac{xm^{1-2\epsilon}}{\log^{9/8-\epsilon} x} \ll \frac{x}{\log^{26/25} x}.$$

The second sum in the error term is bounded since when m is square free, $\varsigma_{a,m^2} \ll \frac{1}{m^2}$. Therefore we have

$$\sum_{m>\log^{1/25} x} \varsigma_{a,m^2} \operatorname{Li}(x) \ll \sum_{m>\log^{1/17} x} \frac{1}{m^2} \operatorname{Li}(x) = O\left(\frac{x}{\log^{26/25} x}\right).$$

For the third sum, we need to show that

$$\sum_{m>\log^{1/25} x} A_a(x,m^2) = O\left(\frac{x}{\log^{26/25} x}\right).$$

Now

$$\sum_{\log^2 x\le m} A_a(x,m^2) \le \sum_{\log^2 x\le m} \#\left\{k\le x \,\middle|\, m^2 \mid k-1\right\} \le \sum_{\log^2 x\le m} \frac{x}{m^2} = O\left(\frac{x}{\log^{26/25} x}\right),$$

while, by the Brun–Titchmarsh Theorem,

$$\begin{aligned}\sum_{\log^{1/25} x<m\le \log^2 x} A_a(x,m^2) &\ll \sum_{\log^{1/25} x<m\le \log^2 x} \pi(x,m^2,1)\\ &\ll \sum_{\log^{1/25} x<m\le \log^2 x} \frac{x}{\varphi(m^2)\log(x/m^2)} = O\left(\frac{x}{\log^{26/25} x}\right).\end{aligned}$$

This completes the proof. □

5. Square free orders: proof of Theorem 1.1

We note that if $n = p_1^{\alpha_1}\cdots p_s^{\alpha_s}$ and $a\in\mathbb{Z}$, then

$$l_n(a) = \text{l.c.m.}(l_{p_1^{\alpha_1}}(a),\cdots, l_{p_s^{\alpha_s}}(a)).$$

Therefore $l_n(a)$ is square free is and only if each $l_{p_i^{\alpha_i}}(a)$ is square free. That is: the function

$$f(n) = \begin{cases}\mu^2(l_n(a)) & \text{if } (n,a)=1;\\ 0 & \text{otherwise}\end{cases}$$

is a multiplicative function of n. We are in the condition to apply the Hypothesis of the Theorem of Wirsing in Lemma 2.2 that are satisfied because of Theorem 1.3, obtaining:

$$I_a(x) = \left(\frac{1}{e^{\gamma\beta_a}\Gamma(\beta_a)} + o(1)\right)\frac{x}{\log x}\prod_{p\le x, p\nmid a}\sum_{\nu=0}^{\infty}\frac{\mu^2(l_{p^\nu}(a))}{p^\nu}.$$

Note that if

$$k_p(a) = \begin{cases} v_p(a^{l_p(a)}-1), & \text{if } p>2;\\ v_2(a^2-1)-1, & \text{if } p=2,\end{cases}$$

then

$$l_{p^\nu}(a) = l_p(a)p^{\max\{0,\nu-k_p(a)\}}.$$

We deduce that $\mu^2(l_{p^\nu}(a))=1$ if and only if $l_p(a)$ is square free and $\nu\le k_p(a)+1$. Therefore

$$\sum_{\nu=0}^{\infty}\frac{\mu^2(l_{p^\nu}(a))}{p^\nu}=1+\frac{\mu^2(l_p(a))}{1-1/p}\left(\frac{1}{p}-\frac{1}{p^{k_p(a)+2}}\right).$$

Hence

$$I_a(x)=\left(\frac{1}{e^{\gamma\beta_a}\Gamma(\beta_a)}\cdot\prod_{\substack{p\nmid a\\ l_p(a)\text{ square free}}}\left(1-\frac{1}{p^{k_p(a)+2}}\right)+o(1)\right)\frac{x}{\log x}\prod_{\substack{p\le x,p\nmid a\\ l_p(a)\text{ square free}}}\left(1-\frac{1}{p}\right)^{-1}.$$

Note that if $\mathcal{J}_a(x)=\{p\le x\,|\,p\nmid a,\ l_p(a)\,\text{square free}\}$, then

$$\begin{aligned}\prod_{p\in\mathcal{J}_a(x)}\left(1-\frac{1}{p}\right)^{-1} &= \exp\left(\sum_{p\in\mathcal{J}_a(x)}\log\left(1-\frac{1}{p}\right)^{-1}\right)\\ &= \exp\left(\sum_{p\in\mathcal{J}_a(x)}\frac{1}{p}\right)+o(1)=(\log x)^{\beta_a}e^{\lambda_a}+o(1).\end{aligned}$$

by partial summation. The constant λ_a is defined by

$$\lambda_a=\lim_{T\to\infty}\sum_{p\in\mathcal{J}_a(T)}\frac{1}{p}-\beta_a\log\log T.$$

Note that the limit exists in virtue of Theorem 1.2 since by partial summation

$$\sum_{p\in\mathcal{J}_a(T)}\frac{1}{p}=-\int_1^T\frac{J_a(t)dt}{t^2}+O\left(\frac{1}{\log T}\right)=\beta_a\log\log T+\lambda_a+O\left(\frac{1}{(\log T)^{1/25}}\right).$$

The constant α_a in Theorem 1.1 is defined by

$$\alpha_a=\frac{1}{e^{\gamma\beta_a-\lambda_a}\Gamma(\beta_a)}\prod_{\substack{p\nmid a\\ l_p(a)\text{ square free}}}\left(1-\frac{1}{p^{k_p(a)+2}}\right)$$

and this completes the proof. □

6. Numerical Data

In this section we compare numerical data. The first table compares the value of the constant β_a with $\frac{J_a(10^7)}{\pi(10^7)}$ for $a=2,3,\dots,22$. Since when $p-1$ is square free necessarily $l_p(a)$ is square free for all a, we always have that

$$\beta_a\ge\prod_l\left(1-\frac{1}{l(l-1)}\right)$$

where $\prod_l\left(1-\frac{1}{l(l-1)}\right)=0.37395\dots$ is the Artin constant. In fact in [5] it is proven that given an integer c, the probability that p is a prime and $p+c$ is k–free equals

$$\prod_l\left(1-\frac{1}{l^{k-1}(l-1)}\right).$$

Finally, the the problem of enumerating primes $p\le x$ in an arithmetic progression for which $p-1$ square free, was addressed in [1].

a	2	3	4	5	6	7	8
$\frac{J_a(10^7)}{\pi(10^7)}$	0.46441	0.51167	0.72989	0.52488	0.54007	0.52794	0.50867
β_a	0.46437	0.51175	0.72972	0.52594	0.54018	0.52788	0.50859
a	9	10	11	12	13	14	15
$\frac{J_a(10^7)}{\pi(10^7)}$	0.65392	0.53349	0.52954	0.51197	0.52997	0.53244	0.53154
β_a	0.65391	0.53359	0.52959	0.51175	0.52991	0.53121	0.53153
a	16	17	18	19	20	21	22
$\frac{J_a(10^7)}{\pi(10^7)}$	0.76299	0.53038	0.46429	0.53030	0.52506	0.53135	0.53110
β_a	0.76289	0.53024	0.46437	0.53034	0.52594	0.53111	0.53126

The following tables compare the values $\varsigma_{a,m}$ (second row) and $\frac{A_a(10^7,m)}{\pi(10^7)}$ (first row) with $a = 2, \ldots, 20$ and $m = 2, \ldots, 21$. Note that the numbers are truncated (not approximated) to the fourth decimal digit.

$a\backslash m$	2	3	4	5	6	7	8	9	10	11
2	0.7081	0.3752	0.4166	0.2082	0.2657	0.1458	0.0832	0.1250	0.1472	0.0915
	0.7083	0.3750	0.4166	0.2082	0.2656	0.1458	0.0833	0.1250	0.1475	0.0916
3	0.6666	0.3747	0.3332	0.2083	0.3123	0.1458	0.1667	0.1251	0.1389	0.0917
	0.6666	0.3750	0.3333	0.2082	0.3125	0.1458	0.1666	0.1250	0.1388	0.0916
4	0.4166	0.3752	0.0832	0.2082	0.1564	0.1458	0.0416	0.1250	0.0866	0.0915
	0.4166	0.3750	0.0833	0.2082	0.1566	0.1458	0.0416	0.1250	0.0868	0.0916
5	0.6664	0.3751	0.3333	0.2082	0.2497	0.1457	0.1667	0.1251	0.0692	0.0915
	0.6666	0.3750	0.3333	0.2082	0.5200	0.1458	0.1666	0.1250	0.0694	0.0916
6	0.6663	0.3750	0.3333	0.2086	0.2656	0.1456	0.1665	0.1250	0.1388	0.0916
	0.6666	0.3750	0.3333	0.2083	0.2656	0.1458	0.1666	0.1250	0.1388	0.0916
7	0.6666	0.3749	0.3333	0.2084	0.2499	0.1456	0.1666	0.1250	0.1390	0.0916
	0.6666	0.3750	0.3333	0.2083	0.2500	0.1458	0.1666	0.1250	0.1388	0.0916

$a\backslash m$	2	3	4	5	6	7	8	9	10	11
8	0.7081	0.1250	0.4166	0.2082	0.0885	0.1458	0.0832	0.0415	0.1472	0.0915
	0.7083	0.1250	0.4166	0.2082	0.0885	0.1458	0.0833	0.0416	0.1475	0.0916
9	0.3332	0.3747	0.1667	0.2083	0.0624	0.1458	0.0832	0.1251	0.0693	0.0917
	0.3333	0.3750	0.1666	0.2082	0.0625	0.1458	0.0833	0.1250	0.0694	0.0916
10	0.6668	0.3749	0.3333	0.2085	0.2498	0.1458	0.1667	0.1249	0.1477	0.0912
	0.6666	0.3750	0.3333	0.2083	0.2500	0.1458	0.1666	0.1250	0.1475	0.0916
11	0.6667	0.3747	0.3333	0.2081	0.2498	0.1457	0.1664	0.1250	0.1386	0.0916
	0.6666	0.3750	0.3333	0.2083	0.2500	0.1458	0.1666	0.1250	0.1388	0.0916
12	0.6665	0.3750	0.3334	0.2081	0.3126	0.1456	0.1667	0.1250	0.1386	0.0917
	0.6666	0.3750	0.3333	0.2082	0.3125	0.1458	0.1666	0.1250	0.1388	0.0916
13	0.6669	0.3748	0.3333	0.2084	0.2499	0.1458	0.1666	0.1251	0.1390	0.0915
	0.6666	0.3750	0.3333	0.2082	0.2500	0.1458	0.1666	0.1250	0.1388	0.0916

$a\backslash m$	2	3	4	5	6	7	8	9	10	11
14	0.6668	0.3751	0.3332	0.2079	0.2503	0.1457	0.1665	0.1248	0.1386	0.0916
	0.6666	0.3750	0.3333	0.2082	0.2500	0.1458	0.1666	0.1250	0.1388	0.0916
15	0.6668	0.3748	0.3332	0.2086	0.2498	0.1457	0.1665	0.1252	0.1391	0.0915
	0.6666	0.3750	0.3333	0.2083	0.2500	0.1458	0.1666	0.1250	0.1388	0.0916
16	0.0832	0.3752	0.0416	0.2082	0.0314	0.1458	0.0209	0.1250	0.0173	0.0915
	0.0833	0.3750	0.0416	0.2082	0.0312	0.1458	0.0208	0.1250	0.0173	0.0916
17	0.6666	0.3749	0.3333	0.2084	0.2502	0.1456	0.1664	0.1249	0.1390	0.0915
	0.6666	0.3750	0.3333	0.2083	0.2500	0.1458	0.1666	0.1250	0.1388	0.0916
18	0.7082	0.3751	0.4165	0.2083	0.2657	0.1457	0.0834	0.1250	0.1475	0.0914
	0.7083	0.3750	0.4166	0.2082	0.2656	0.1458	0.0833	0.1250	0.1475	0.0916
19	0.6666	0.3750	0.3332	0.2083	0.2500	0.1457	0.1667	0.1250	0.1386	0.0917
	0.6666	0.3750	0.3333	0.2083	0.2500	0.1458	0.1666	0.1250	0.1388	0.0916
20	0.6667	0.3751	0.3334	0.2082	0.2500	0.1459	0.1666	0.1248	0.0693	0.0914
	0.6666	0.3750	0.3333	0.2083	0.2500	0.1458	0.1666	0.1250	0.0694	0.0916

$a\backslash m$	12	13	14	15	16	17	18	19	20	21
2	0.1564	0.0774	0.1031	0.0781	0.0416	0.0590	0.0885	0.0526	0.0866	0.0546
	0.1562	0.0773	0.1032	0.0781	0.0416	0.0590	0.0885	0.0527	0.0868	0.0546
3	0.0624	0.0775	0.0971	0.0782	0.0832	0.0589	0.1044	0.0526	0.0693	0.0546
	0.0625	0.0773	0.0972	0.0781	0.0833	0.0590	0.1041	0.0527	0.0694	0.0546
4	0.0314	0.0774	0.0605	0.0781	0.0209	0.0590	0.0521	0.0526	0.0173	0.0546
	0.0315	0.0773	0.0607	0.0781	0.0208	0.0590	0.0520	0.0527	0.0173	0.0546
5	0.1249	0.0774	0.0970	0.0781	0.0832	0.0588	0.0834	0.0525	0.0346	0.0545
	0.1250	0.0773	0.0972	0.0781	0.0833	0.0590	0.0833	0.0527	0.0347	0.0546
6	0.1563	0.0772	0.0971	0.0783	0.0832	0.0589	0.0885	0.0525	0.0693	0.0546
	0.1562	0.0773	0.0972	0.0781	0.0833	0.0590	0.0885	0.0527	0.0694	0.0546
7	0.1250	0.0775	0.1213	0.0781	0.0832	0.0589	0.0833	0.0527	0.0693	0.0547
	0.1250	0.0773	0.1215	0.0781	0.0833	0.0590	0.0833	0.0527	0.0694	0.0546

$a\backslash m$	12	13	14	15	16	17	18	19	20	21
8	0.0521	0.0774	0.1031	0.0260	0.0416	0.0590	0.0294	0.0526	0.0866	0.1823
	0.0520	0.0773	0.1032	0.0260	0.0416	0.0590	0.0295	0.0527	0.0868	0.1822
9	0.0313	0.0775	0.0485	0.0782	0.0416	0.0589	0.0208	0.0526	0.0347	0.0546
	0.0312	0.0773	0.0486	0.0781	0.0416	0.0590	0.0208	0.0527	0.0347	0.0546
10	0.1250	0.0774	0.0972	0.0783	0.0833	0.0589	0.0831	0.0527	0.0871	0.0546
	0.1250	0.0773	0.0972	0.0781	0.0833	0.0590	0.0833	0.0527	0.0868	0.0546
11	0.1248	0.0773	0.0971	0.0782	0.0833	0.0590	0.0833	0.0526	0.0693	0.0545
	0.1250	0.0773	0.0972	0.0781	0.0833	0.0590	0.0833	0.0527	0.0694	0.0546
12	0.0625	0.0775	0.0971	0.0781	0.0832	0.0590	0.1042	0.0526	0.0693	0.0547
	0.0625	0.0773	0.0972	0.0781	0.0833	0.0590	0.1041	0.0527	0.0694	0.0546
13	0.1251	0.0775	0.0973	0.0779	0.0831	0.0589	0.0834	0.0526	0.0695	0.0545
	0.1250	0.0773	0.0972	0.0781	0.0833	0.0590	0.0833	0.0527	0.0694	0.0546

$a\backslash m$	12	13	14	15	16	17	18	19	20	21
14	0.1252	0.0774	0.1032	0.0778	0.0832	0.0589	0.0832	0.0526	0.0691	0.0546
	0.1250	0.0773	0.1032	0.0781	0.0833	0.0590	0.0833	0.0527	0.0694	0.0546
15	0.1249	0.0772	0.0970	0.0782	0.0832	0.0589	0.0834	0.0525	0.0696	0.0544
	0.1250	0.0773	0.0972	0.0781	0.0833	0.0590	0.0833	0.0527	0.0694	0.0546
16	0.0156	0.0774	0.0121	0.0781	0.0104	0.0590	0.0104	0.0526	0.0086	0.0546
	0.0156	0.0773	0.0121	0.0781	0.0104	0.0590	0.0104	0.0525	0.0086	0.0546
17	0.1249	0.0773	0.0972	0.0782	0.0831	0.0590	0.0834	0.0525	0.0695	0.0546
	0.1250	0.0773	0.0972	0.0781	0.0833	0.0590	0.0833	0.0527	0.0694	0.0546
18	0.1563	0.0774	0.1030	0.0782	0.0416	0.0589	0.0884	0.0527	0.0867	0.0549
	0.1562	0.0773	0.1032	0.0781	0.0416	0.0590	0.0885	0.0527	0.0868	0.0546
19	0.1249	0.0772	0.0972	0.0783	0.0835	0.0590	0.0833	0.0526	0.0691	0.0545
	0.1250	0.0773	0.0972	0.0781	0.0833	0.0590	0.0833	0.0527	0.0694	0.0546
20	0.1251	0.0773	0.0972	0.0783	0.0832	0.0588	0.0832	0.0525	0.0346	0.0547
	0.1250	0.0773	0.0972	0.0781	0.0833	0.0590	0.0833	0.0527	0.0347	0.0546

7. k–free orders

We recall that an integer is said to be *k–free* if it is not divisible by the k-th power of any prime number.

Let $\mathcal{S}_k$ is the set of integers which are k-free. The same argument as in Theorem 1.2 gives

$$\#\{p \le x \,|\, p \nmid a,\ l_p(a) \in \mathcal{S}_k\} \sim \beta_{a,k}\,\mathrm{Li}(x)$$

where, for $k \ge 3$,

$$\beta_{a,k} = \left[\prod_{l}\left(1 - \frac{1}{l^{k+v_l(h)-2}(l^2-1)}\right)\right] \cdot \left[1 - \frac{1}{2}\prod_{l|[2,a_1]} \frac{1}{1 - l^{k+v_l(h)-2}(l^2-1)}\right].$$

We will omit the proof. A similar statement as Theorem 1.1 also holds.

Acknowledgements: The author would like to thank Igor Shparlinski for having inspired him the paper and for his constant support during the redaction. Furthermore the author would like to thank John Friedlander, Carl Pomerance and Igor Shparlinski for having suggested to use the Rankin method to prove Lemma 3.3. Finally the author would like to thank Andrew Granville for his precious help in polishing and highly simplifying several of the proofs, Pieter Moree for some suggestions and for pointing out reference [11].

References

[1] L.M. Adleman, C. Pomerance and R.S. Rumely, *On distinguishing prime numbers from composite numbers*. Ann. of Math. (2) **117** (1983), 173–206.

[2] K. Chinen and L. Murata, *On a distribution property of the residual order of* $a(\bmod p)$ *I, II*. *Preprint* 2002.

[3] J. von zur Gathen and F. Pappalardi, *Density Estimates related to Gauss periods*. Lam, Kwok-Yan (ed.) et al., Cryptography and computational number theory. Proceedings of the workshop, CCNT'99, Singapore, November 22-26, 1999. Basel: Birkhäuser. Prog. Comput. Sci. Appl. Log. 2001 **20**, 33-41.

[4] C. Hooley, *On Artin's Conjecture*. J. Reine Angew. Math.**226** (1967), 207–220.

[5] L. Mirsky, *The number of representations of an integer as the sum of a prime and a* k*-free integer*. Amer. Math. Monthly **56** (1949), 17–19.

[6] J. C. Lagarias and A. M. Odlyzko, *Effective versions of the Chebotarev Density Theorem*. In Algebraic Number Fields, Ed. A. Fröhlich. Academic press, New York, 1977, 409–464.

[7] P. Moree, *On the distribution of the order and index of* $g(\mathrm{mod} p)$ *over residues classes*. *Preprint* 2002.

[8] R. W. K. Odoni, *A conjecture of Krishnamurthy on decimal periods and some allied problems*. J. Number Theory **13** (1981), 303–319.

[9] F. Pappalardi, *On Hooley's theorem with weights*. Rend. Sem. Mat. Univ. Pol. Torino **53** (1995), 375–388.

[10] F. Pappalardi, F. Saidak and I. Shparlinski, *Squarefree Values of the Carmichael Function*. *Preprint* 2002.

[11] K. Wiertelak, *On the density of some sets of primes* p*, for which* $n \mid \mathrm{ord}_p a$. Funct. Approx. Comment. Math. **28** (2000), 237–241.

[12] E. Wirsing, *Das asymptotische Verhalten von Summen über multiplikative Funktionen*. Math. Ann. **143** (1961), 75–102.

Dipartimento di Matematica, Università degli Studi Roma Tre, Largo S. L. Murialdo 1, Roma, 00146, Italy

E-mail address: pappa@mat.uniroma3.it