ACTA ARITHMETICA
174.4 (2016)

Upper bounds for the number of primitive ray class characters with conductor below a given bound

by

Joshua Zelinsky (Orono, ME)

1. Introduction. Fix a positive integer a, and write $\mathrm{ord}_n(a)$ for the order of a in the multiplicative group of invertible residue classes modulo n when $(a,n)=1$. Let

$$G(x) = \sum_{n\le x,\,(n,a)=1} \frac{\phi(n)}{\mathrm{ord}_n(a)}.$$

We show that for any α we have $G(x) = O(x^2/\log^\alpha x)$. The motivation for investigating these sums stems from two distinct problems: the Artin primitive root conjecture and the problem of counting Artin representations.

Artin conjectured that for any given rational integer a, $a \neq 1$ and a not a perfect square, the set rational primes p such that a is a primitive root modulo p has positive density and he conjectured a formula for that density. Major work on Artin's conjecture is due to Hooley [Hool], Murty and Gupta [GM], and Heath-Brown [H-B]. Since then, work has been done generalizing the Artin conjecture in a variety of directions. Our result concerning $G(x)$ represents one such direction. Instead of confining ourselves to prime moduli, we also consider composite moduli, and instead of considering moduli for which a is of maximal order, we consider the average order of the index of the cyclic group generated by the residue class of a. There is an earlier paper similar in theme to this paper's approach by Murty and Srinivasan [MS].

Our second motivating problem, that of counting Artin representations, is actually connected not with $G(x)$ itself but rather with a closely related sum over number fields. Let K be a number field with ring of integers O_K. Let U_K be the set of units of O_K, and for any ideal I let $U_K(I)$ be the

2010 *Mathematics Subject Classification*: Primary 11N56; Secondary 11R65.
Key words and phrases: Artin representations, primitive roots.
Received 1 July 2013; revised 9 May 2016.
Published online 3 August 2016.

DOI: 10.4064/aa7506-5-2016

subgroup of U_K formed by elements which are 1 (mod I). Let $U_K(I)^+$ be the subgroup of $U_K(I)$ formed by elements which are positive in all real embeddings of K. Let

$$P_K(x) = \sum_{\mathbf{N}I \leq x} \frac{\phi(I)}{[U_K : U_K(I)]}$$

with the sum over non-zero ideals of O_K. Assume that the unit group of O_K has positive rank. Then for any α, we have $P_K(x) = O(x^2/\log^\alpha x)$. We remark that P_K represents an analog of G for number fields.

Let us now explain the connection between these sums and the problem of estimating the number of Artin representations of fixed dimension, fixed base field, and conductor of bounded norm. We focus on the case of dimension 1, so one is essentially counting primitive ray class characters. Let K be a number field and let $\delta_{K,1}(x)$ count the number of 1-dimensional Artin representations up to isomorphism with norm of the conductor at most x. Rohrlich [Rohr] has noted the elementary estimate $\delta_{K,1}(x) = O(x^2)$, and if K is the rationals or a quadratic imaginary field, then this is the correct order of growth and one can in fact produce an asymptotic formula, with the constant depending on the field. The method of proof is to note that

$$\delta_{K,1}(x) \leq \sum_{\mathbf{N}I \leq x} h_K^{\mathrm{nar}}(I)$$

where $h_K^{\mathrm{nar}}(I)$ is the order of the narrow ray class group of K with modulus I. In fact,

$$\delta_{K,1}(x) = \sum_{\mathbf{N}I \leq x} \sum_{Q|I} \mu\left(\frac{I}{Q}\right) h_K^{\mathrm{nar}}(Q)$$

where μ is the generalization of the Möbius function to ideals.

One has (see [L2])

$$h_K^{\mathrm{nar}}(I) = \frac{2^{r_1} h_K \phi(I)}{[U_K : U_K{}^+(I)]}.$$

Note that $[U_K : U_K{}^+(I)]$ and $[U_K : U_K(I)]$ differ by at most a power of 2, the maximum exponent of which is bounded in terms of the rank of the unit group of the field. Thus, estimating $P_K(x)$ gives us information about the number of Artin representations, since the other parts in the formula for the order of the narrow class group all depend only on K. Prior to this work, lower bounds for both $P(x)$ and $G(x)$ have been obtained by Ambrose [Ambr], who also conjectured that for both functions, the correct growth order is $x^{2+o(1)}$. The estimates for $G(x)$ and $P_K(x)$ are similar, as one can think of $G(x)$ as the analog to $P_K(x)$ in the S-integers with S equal to the set of prime divisors of a, but the proofs are presented separately; it

is likely that a framework can be constructed which subsumes both results into a single proof, but as of yet, attempts at such an approach lead to technical difficulties.

Note that while this paper was under review, Sungjin Kim [Kim] used a method of Pomerance to obtain a better bound than that appearing here. It is likely that Kim's method along with some of the techniques in this paper can be combined to obtain a bound which is stronger than either.

2. Over the rational integers. We will first collect some technical lemmas needed for our proofs. We will write $\omega(n)$ to be the number of distinct prime divisors of n. When we move to the case over number fields, we will write $\omega(I)$ for the number of distinct prime ideals dividing an ideal I.

LEMMA 2.1. *If* $2 \le y \le x/2$, *then*

$$\frac{x^x}{(x-y)^{x-y}} < e^{2y}x^y.$$

Proof. Consider

$$\log \frac{x^x}{(x-y)^{x-y}} = x\log x - (x-y)\log(x-y) = x\left(\log x - \left(1-\frac{y}{x}\right)\log(x-y)\right).$$

We have

$$x\left(\log x - \left(1-\frac{y}{x}\right)\log(x-y)\right) < x\left(\log\frac{x}{x-y} + \frac{y\log x}{x}\right).$$

Set $u = x/(x-y) - 1 = y/(x-y)$. Since $y \le x/2$ and $\log(1+u) \le u$ we have $\log x/(x-y) \le 2y/x$. Thus

$$\log \frac{x^x}{(x-y)^{x-y}} \le x\left(\frac{2y}{x} + \frac{y\log x}{x}\right) = 2y + y\log x,$$

so exponentiating now gives the desired result. ∎

LEMMA 2.2. *If* $1 \le j \le (k-2)/3$, *then*

$$\binom{k}{j} \le \frac{\binom{k}{j+1}}{2}.$$

Proof. Note that $\binom{k}{j}/\binom{k}{j+1} = (j+1)/(k-j)$. We have $(j+1)/(k-j) \le 1/2$ when $j \le (k-2)/3$. ∎

LEMMA 2.3. *If* $2 \le m \le (k-2)/3$, *then*

$$\sum_{j=1}^{m}\binom{k}{j} \le \left(\frac{e^2k}{m}\right)^m.$$

Proof. We will first estimate $\binom{k}{m}$ and then use Lemma 2.2 to bound $\sum_{j=1}^{m}\binom{k}{j}$. We require the following version of Stirling's formula, valid for

$n \geq 2$:

$$\sqrt{2\pi n}\left(\frac{n}{e}\right)^n e^{\frac{1}{12n+1}} < n! < \sqrt{2\pi n}\left(\frac{n}{e}\right)^n e^{\frac{1}{12n}}$$

(see for example [L1]). We have

$$\frac{k!}{m!(k-m)!} < \frac{\sqrt{2\pi k}\left(\frac{k}{e}\right)^k e^{\frac{1}{12k}}}{\sqrt{2\pi m}\left(\frac{m}{e}\right)^m \sqrt{2\pi(k-m)}\left(\frac{k-m}{e}\right)^{k-m} e^{\frac{1}{12m+1}} e^{\frac{1}{12(k-m)+1}}}.$$

Since $m < k$, we obtain

$$\binom{k}{m} < \frac{\sqrt{k}\, k^k}{\sqrt{m} m^m \sqrt{2\pi(k-m)}\,(k-m)^{k-m}}.$$

By Lemma 2.1 with $x = k$ and $y = m$, we have $k^k/(k-m)^{k-m} < e^{2m}k^m$, and thus

$$\binom{k}{m} < \frac{e^{2m}k^m\sqrt{k}}{m^m\sqrt{m}\sqrt{2\pi(k-m)}}.$$

Since $m \leq (k-2)/3 < k/2$, we see that $k - m > k/2$ and so

$$\binom{k}{m} < \frac{e^{2m}k^m\sqrt{k}}{m^m\sqrt{m}\sqrt{\pi k}} = \frac{e^{2m}k^m}{\sqrt{m}\sqrt{\pi}\, m^m}.$$

By Lemma 2.2, we obtain

$$\sum_{j=1}^{m}\binom{k}{j} \leq \binom{k}{m} + \frac{\binom{k}{m}}{2} + \frac{\binom{k}{m}}{4} + \cdots = 2\binom{k}{m} < 2\frac{e^{2m}k^m}{\sqrt{m}\sqrt{\pi}\, m^m}.$$

Since $m \geq 2$, we find that $2/\sqrt{\pi m} < 1$, so we are done. ∎

Lemma 2.4. *Let $\epsilon > 0$ and let $D_\epsilon(x)$ be the number of positive integers with $\omega(n)$ for $n \leq x$ satisfying $\omega(n) \geq (\log x)^\epsilon$. Then for all $\alpha > 0$,*

$$D_\epsilon(x) = O\left(\frac{x}{(\log x)^\alpha}\right).$$

Proof. We have $\sum_{n\leq x}\tau(n) = O(x\log x)$ where $\tau(n)$ is the number of positive divisors of n. Note that $\tau(n) \geq 2^{\omega(n)}$ for all n. If $\omega(n) \geq (\log x)^\epsilon$, then

$$\tau(n) \geq 2^{(\log x)^\epsilon}.$$

Thus, $D_\epsilon 2^{(\log x)^\epsilon} = O(x\log x)$, from which the result follows. ∎

Theorem 2.5. *For any α, we have*

$$G(x) = O\left(\frac{x^2}{(\log x)^\alpha}\right).$$

Proof. We will prove the equivalent result that for any fixed $\alpha > 1$,

$$G(x) = O\left(\frac{x^2(\log\log x)^2}{(\log x)^\alpha}\right).$$

Let $S(x)$ be the set of $n \le x$ with $(n, a) = 1$. Define $S(x, p, q)$ to be the subset of $S(x)$ with $p \le \operatorname{ord}_n(a) \le q$. Set $t = (\log x)^\alpha$. Note that if x is sufficiently large, then $t > 3\log_a x$. Write $\ell(x) = 3\log_a x$. Here by $\log_a x$ we mean $\log x/\log a$ rather than the a-fold logarithm. Then

$$G(x) \le \mathrm{I}(x) + \mathrm{II}(x) + \mathrm{III}(x) \tag{2.1}$$

where

$$\mathrm{I}(x) = \sum_{n\in S(x,1,\ell(x))} \frac{n}{\operatorname{ord}_n(a)}, \tag{2.2}$$

$$\mathrm{II}(x) = \sum_{n\in S(x,\ell(x),t)} \frac{n}{\operatorname{ord}_n(a)}, \tag{2.3}$$

$$\mathrm{III}(x) = \sum_{n\in S(x,t,\infty)} \frac{n}{\operatorname{ord}_n(a)}. \tag{2.4}$$

We will estimate each of these sums separately.

The easiest are $\mathrm{I}(x)$ and $\mathrm{III}(x)$. $\mathrm{I}(x)$ has at most $\sum_{1\le r\le\ell(x)} \tau(a^r - 1)$ terms. We have

$$\sum_{1\le r\le\ell(x)} \tau(a^r - 1) \le \ell(x)\tau_m(x)$$

where $\tau_m(x)$ is the maximum of $\tau(a^r - 1)$ with r ranging from 1 to $\ell(x)$. Since $\tau(n) = O(n^\epsilon)$ for any $\epsilon > 0$, $\tau_m(x) = O(x^\epsilon)$. Any term in $\mathrm{I}(x)$ is bounded above by x, and so we conclude that $\mathrm{I}(x) = O(x^\epsilon\ell(x)x) = O(x^{1+\epsilon}\log x)$. Thus in fact, for any $\epsilon > 0$ we have $\mathrm{I}(x) = O(x^{1+\epsilon})$.

Next, we need to estimate $\mathrm{III}(x)$. In this case we use the fact that it has at most x terms and each term is at most x/t and so $\mathrm{III}(x) \le x^2/t$.

To estimate $\mathrm{II}(x)$ we need some preliminary remarks.

Given any $\epsilon > 0$, we have $\omega(n) < (1 + \epsilon)\log n/\log\log n$ for all but finitely many n. For simplicity, we take $\epsilon = 1$ and so for all but finitely many n we have $\omega(n) < 2\log n/\log\log n$. Let N be the set of d such that $(a, d) = 1$ and $d \mid n$ for some n satisfying $\omega(n) \ge 2\log n/\log\log n$. Note that N is finite; hence

$$\sum_{n\in N,\, n\le x} \frac{\phi(n)}{\operatorname{ord}_n(a)} = O(1).$$

Let β be a real number with $0 < \beta < 1$, let $H(x)$ be the subset of elements of $S(x, \ell(x), t) \setminus N$ with at most $(\log x)^\beta$ distinct prime factors, and set

$$\mathrm{II}_1(x) = \sum_{n\in H(x)} \frac{n}{\operatorname{ord}_n(a)}. \tag{2.5}$$

Similarly, let $J(x)$ be the elements with more than $(\log x)^\beta$ distinct prime factors and not in N, and set

$$\text{II}_2(x) = \sum_{n \in J(x)} \frac{n}{\text{ord}_n(a)}. \tag{2.6}$$

Thus, $\text{II}(x) = \text{II}_1(x) + \text{II}_2(x) + O(1)$. So we need only bound $\text{II}_1(x)$ and $\text{II}_2(x)$.

For $\text{II}_1(x)$, we need to estimate $H(x)$. If $d \in H(x)$, then $d \mid a^r - 1$ with $\ell(x) \le r \le t$. So we need to estimate how many divisors $a^r - 1$ can have which are less than or equal to x and not in N. Note that the number of prime factors of $a^r - 1$ is bounded by

$$\omega(a^r - 1) \le \frac{2 \log a^r}{\log \log a^r} \le \frac{(3 \log a) r}{\log r} \le t.$$

The last inequality above is valid for sufficiently large values of t. Recall that t grows with x.

Thus, each $a^r - 1$ whose divisors contribute to $H(x)$ has at most t distinct prime divisors. However, each element in $H(x)$ has j distinct prime divisors, for some j satisfying $1 \le j \le (\log x)^\beta$. So for any given r, there are at most $\sum_{j=1}^{m} \binom{k}{j}$ possible choices for the distinct prime divisors where k is the largest integer $\le t = (\log x)^\alpha$ and m is the largest integer $\le (\log x)^\beta$. Any prime factor of such a divisor can be raised to at most the $\log_2 x$ power, so the total number of divisors is bounded by $\left(\sum_{j=1}^{m} \binom{k}{j}\right) (\log_2 x)^{(\log x)^\beta}$. There are at most t possible values of r. Thus,

$$|H(x)| \le t \sum_{j=1}^{m} \binom{k}{j} (\log_2 x)^{(\log x)^\beta}.$$

Applying Lemma 2.3 and using the values of k and m then gives

$$|H(x)| \le t \left(\frac{e^2 t}{(\log x)^\beta} \right)^{(\log x)^\beta} (\log_2 x)^{(\log x)^\beta}.$$

(Again, by $\log_2 x$ we mean $\log x / \log 2$.) We can replace the floor of $(\log x)^\beta$ with $(\log x)^\beta$ since $(e^2 t/s)^s$ is an increasing function in s when s is small compared to t.

Thus we have

$$\log |H(x)| \le C (\log x)^\beta (\log \log x) + \log t + (\log \log_2 x)(\log x)^\beta$$

for some constant C, and this is $O((\log x)^\beta \log \log x)$. Since $\beta < 1$ we conclude that $|H(x)| = O(x^{\epsilon_0})$, and so $\text{II}_1(x) = O(x^{1+\epsilon_0})$ for any $\epsilon_0 > 0$ since the terms in $\text{II}_1(x)$ are at most x.

To estimate $\mathrm{II}_2(x)$ we apply Lemma 2.4, so that the number of terms of J is $O(x/(\log x)^{k\beta})$ for any k, and thus we conclude that

$$\mathrm{II}_2(x) = O\left(\frac{x^2}{(\log x)^k}\right)$$

for any k since every term in $\mathrm{II}_2(x)$ is at most $x/\ell(x)$. ∎

3. Number fields. Let K be a number field and let O_K be its ring of integers. Set $d = [K : \mathbb{Q}]$. Define $\omega(I)$ to be the number of distinct prime ideal divisors of I, where I is an ideal of O_K. Define $j_K(x) = \sum_{\mathbf{N}I \le x} \omega(I)^2$ and $\tau(I) = \sum_{A|I} 1$ (that is, $\tau(I)$ counts the number of ideals which divide I).

LEMMA 3.1. $\sum_{\mathbf{N}I \le x} \tau(I) = O(x \log x)$.

Versions of this lemma can be found in some number theory textbooks such as [Nar, Chap. 7] using the zeta function of the number field. We include a proof below for completeness and because it is worth noting that a purely elementary proof of the statement can be provided.

Proof of Lemma 3.1. We may rewrite $\sum_{\mathbf{N}I \le x} \tau(I)$ as

$$\sum_{\mathbf{N}I \le x} L\left(\frac{x}{\mathbf{N}I}\right)$$

where $L(x)$ counts the number of ideals with norm at most x. Since $L(x) \sim cx$ for some constant c, we have $L(x) = O(x)$, and thus

$$\sum_{\mathbf{N}I \le x} L\left(\frac{x}{\mathbf{N}I}\right) = O\left(\sum_{\mathbf{N}I \le x} \frac{x}{\mathbf{N}I}\right).$$

Since $L(x) \sim cx$, if we list the ideals of O_K in the order of increasing norm, as I_n (without paying attention to the order when the ideals have the same norm), then we must have a constant c_0 such that $I_i > c_0 i$ for all sufficiently large i. Thus,

$$\sum_{\mathbf{N}I \le x} \left(\frac{x}{\mathbf{N}I}\right) = O\left(\sum_{i \le x} \frac{x}{i}\right)$$

which gives the desired result. ∎

LEMMA 3.2. *For $\beta > 0$, let $D_\beta(x)$ be the number of ideals I with $\omega(I) \ge (\log x)^\beta$ and $\mathbf{N}I \le x$. Then for any fixed β and any $\gamma > 0$ we have $D_\beta(x) = O(x/(\log x)^\gamma)$, where the implied constant depends on β and γ.*

Proof. This follows essentially by the same method of proof as in Lemma 2.4 by noting that $\tau(I) \ge 2^{\omega(I)}$. ∎

Henceforth, we will assume that O_K has a unit a of infinite order (that is, K is not the rationals or a quadratic imaginary field).

LEMMA 3.3. *For any a in $O_K^\times$, there exists a constant $C > 1$ such that for all k,*

$$|N_{K/\mathbb{Q}}(a^k - 1)| \leq C^k.$$

Proof. We may take C to be 1 plus the absolute value of the product of all the conjugates of a. ∎

For any ideal I of O_K let $o_a(I)$ be the smallest positive integer such that $I \mid (a^{o_a} - 1)$. So, o_a is the order of a in the group $(O_K/I)^\times$.

LEMMA 3.4. *There is a constant $C > 1$ depending on K and a such that for any ideal I of O_K we have $o_a(I) \geq \log_C \mathbf{N}I$.*

Proof. Assume that $I \mid (a^k - 1)$. So $\mathbf{N}I \leq \mathbf{N}(a^k - 1) = |N_{K/\mathbb{Q}}(a^k - 1)|$ since $(a^k - 1)$ is a principal ideal. By Lemma 3.3, there is a constant $C > 1$ depending only on a such that $|N_{K/\mathbb{Q}}(a^k - 1)| \leq C^k$, from which the result follows. ∎

COROLLARY 3.5. *Assume that the group of units of O_K has positive rank. Then there is a constant $C > 1$ such that $[U_K : U_K(I)] \geq \log_C \mathbf{N}I$.*

Proof. Apply Lemma 3.4, and note that if a is a unit of infinite order, then $I \mid (u^{[U_K:U_K(I)]} - 1)$. ∎

LEMMA 3.6. *For all but finitely many ideals I, we have*

$$\omega(I) < 2d \frac{\log \mathbf{N}I}{\log\log \mathbf{N}I}.$$

Moreover, if $\tau(I)$ is the number of distinct ideal divisors of I then $\tau(I) = O((\mathbf{N}I)^\epsilon)$ for any $\epsilon > 0$.

Proof. Recall that for any $\epsilon > 0$ and for all but finitely many n we have $\omega(n) < (1 + \epsilon)\log n/\log\log n$. As before, we will take $\epsilon = 1$, and so for all but finitely many n, $\omega(n) < 2\log n/\log\log n$. Let N be the set of positive integers violating the prior inequality, and let M be the set of ideals with norm in N or with norm less than or equal to e^e. Note that since N is finite, so is M. Let C_M be the maximum number of distinct prime divisors of any element of M.

Now, for any given ideal I, set $I_0 = \mathrm{rad}(I)$ to be the largest squarefree ideal divisor of I.

So we need to just estimate $\omega(I_0)$. If $I_0 \in M$, then $\omega(I_0) \leq C_M$. If $I_0 \notin M$, then since any prime in $\mathbb{Z}$ factors into at most d distinct prime ideals in K, we have

$$\omega(I_0) \leq \frac{2d\log \mathbf{N}I_0}{\log\log \mathbf{N}I_0} \leq \frac{2d\log \mathbf{N}I}{\log\log \mathbf{N}I}.$$

The last inequality follows from the fact that for $x > e^e$, $\log x/\log\log x$ is an increasing function.

To prove the result for $\tau(I)$, note that $\tau(n) = O(n^\epsilon)$ and it suffices to prove that there is a constant m such that

$$\tau(I) = o(\tau(\mathbf{N}I)^m),$$

which we only need to prove for ideals whose norm is a power of a prime since $\tau(I)$ is a multiplicative function. Assume that $\mathbf{N}I = p^a$, so that $\tau(\mathbf{N}I) = a+1$. Then the number of divisors of I is bounded by the number of solutions in non-negative integers to the inequality

$$x_1 + \cdots + x_d \le a + 1,$$

which is $(a + d + 1)!/(d!(a + 1)!)$. Since $d = [K : \mathbb{Q}]$ is fixed, the result follows. ∎

THEOREM 3.7. *For any α we have $P_K(x) = O(x^2/(\log x)^\alpha)$.*

Proof. The proof is similar to our earlier estimate for $G(x)$.

We will show the equivalent result that for any fixed α such that $1 < \alpha$, we have $P_K(x) = O(x^2(\log\log x)^2/(\log x)^\alpha)$.

We will write $\mathrm{ord}(I)$ to be the smallest positive integer o such that $a^o - 1$ is in I. We note that

$$P_K(x) \le \sum_{\mathbf{N}I \le x} \frac{\mathbf{N}I}{\mathrm{ord}(I)}.$$

Let C be the constant from Lemma 3.4. Also, let $\ell(x) = 3\log_C x$, and set $t = (\log x)^\alpha$.

We set $T(x, p, q)$ to be those I with norm at most x and satisfying $p \le \mathrm{ord}(I) < q$. Then

$$P_K(x) \le \mathrm{I}(x) + \mathrm{II}(x) + \mathrm{III}(x)$$

where we have sums defined in an analogous fashion as earlier:

$$\mathrm{I}(x) = \sum_{I \in T(x,1,\ell(x))} \frac{\mathbf{N}I}{\mathrm{ord}(I)}, \tag{3.1}$$

$$\mathrm{II}(x) = \sum_{I \in T(x,\ell(x),t)} \frac{\mathbf{N}I}{\mathrm{ord}(I)}, \tag{3.2}$$

$$\mathrm{III}(x) = \sum_{I \in T(x,t,\infty)} \frac{\mathbf{N}I}{\mathrm{ord}(I)}. \tag{3.3}$$

We will first estimate $\mathrm{I}(x)$. The number of terms in $\mathrm{I}(x)$ is bounded by $\sum_{1 \le r \le \ell(x)} \tau((a^r - 1))$. This sum is at most $\ell(x)\tau_m(x)$ where $\tau_m(x)$ is the maximum of $\tau((a^r - 1))$ over r satisfying $1 \le r \le \ell(x)$. By Lemma 3.6 we have $\tau_m(I) = O(x^\epsilon)$. Any term in $\mathrm{I}(x)$ is bounded above by x and so

$$\mathrm{I}(x) = O(x^{1+\epsilon} 3(\log_c x)) = O(x^{1+\epsilon}\log x).$$

Since $\log x = o(x^\epsilon)$ for any $\epsilon > 0$ we conclude that

$$\mathrm{I}(x) = O(x^{1+\epsilon}).$$

Next, we estimate $\mathrm{III}(x)$. It has at most $O(x)$ terms (since the number of ideals of norm at most x is $O(x)$) and each term is at most x/t and so

$$\mathrm{III}(x) = O\left(\frac{x^2}{t}\right) = O\left(\frac{x^2}{(\log x)^\alpha}\right).$$

To estimate $\mathrm{II}(x)$ we will break it into two sets of terms depending on how many distinct prime factors J has, along with an $O(1)$ as before.

Let k be a constant that satisfies Lemma 3.6. We define N_k to be the set of ideals which divide some J with $\omega(J) \geq C \log \mathbf{N}J/\log\log \mathbf{N}$. Note that N_k is finite.

Fix a real number β with $0 < \beta < 1$. Let $H(x)$ be the subset of elements of $T(x, \ell(x), t)$ with are not in N_k and which have at most $(\log x)^\beta$ distinct prime factors, and set

$$\mathrm{II}_1(x) = \sum_{I \in H(x)} \frac{\mathbf{N}I}{\mathrm{ord}(I)}. \tag{3.4}$$

Similarly, let $J(x)$ be the set of elements of $T(x, \ell(x), t)$ with more than $(\log x)^\beta$ distinct prime ideal factors, and not in N_j, and set

$$\mathrm{II}_2(x) = \sum_{I \in J(x)} \frac{\mathbf{N}I}{\mathrm{ord}(I)}. \tag{3.5}$$

To estimate $\mathrm{II}_1(x)$ we will estimate $|H(x)|$. If $I \in H(x)$ then $I \,|\, (a^r - 1)$ for some r with $\ell(x) \leq r \leq t$ and $(a^r - 1)$ not in N_k. Then by Corollary 3.5 and Lemma 3.6 we have, for some constant M,

$$\omega((a^r - 1)) < \frac{Mr}{\log r} < t.$$

The last inequality is valid for t sufficiently large, which occurs when x is sufficiently large. However, each element of $|H(x)|$ has j distinct prime divisors with $1 \leq j \leq (\log x)^\beta$. So for any fixed r, there are at most $\sum_{j=1}^m \binom{k}{j}$ possible choices for the distinct prime divisors where k is the largest integer $\leq t$ and m is the largest integer $\leq (\log x)^\beta$. Any prime can be raised to at most the $\log_2 x$ power, so the total number of divisors is bounded by $\left(\sum_{j=1}^m \binom{k}{j}\right)(\log_2 x)^{(\log x)^\beta}$. There are at most t possible values of r. Thus,

$$|H(x)| \leq \sum_{j=1}^m \binom{k}{j} t (\log_2 x)^{(\log x)^\beta}.$$

Applying Lemma 2.3 and using the values of k and m then gives

$$|H(x)| \le t\left(\frac{e^2 t}{(\log x)^\beta}\right)^{(\log x)^\beta} (\log_2 x)^{(\log x)^\beta}.$$

Now, since $t = (\log x)^\alpha$,

$$\log|H(x)| \le C(\log x)^\beta \log\log x + \log t + (\log\log_2 x)(\log x)^\beta$$

for some constant C, and this is $O((\log x)^\beta \log\log x)$. Thus $|H(x)| = O(x^{\epsilon_0})$, and so $\mathrm{II}_1(x) = O(x^{1+\epsilon_0})$ for any $\epsilon_0 > 0$.

To estimate $\mathrm{II}_2(x)$, apply Lemma 3.2 so that the number of terms of $J(x)$ is $O(x(\log\log x)^2/(\log x)^\gamma)$ for any $\gamma > 0$, and thus conclude that

$$\mathrm{I}_2(x) = O\left(\frac{x^2(\log\log x)^2}{(\log x)^\gamma}\right)$$

for every γ. ∎

Acknowledgements. We thank Nigel Pitt, Rob Pollack, David Rohrlich, Glenn Stevens, and Eve Zelinsky.

We would also like to acknowledge the anonymous first referee's very helpful comments.

References

[Ambr] C. Ambrose, *Artin's primitive root conjecture and a problem of Rohrlich*, Math. Proc. Cambridge Philos. Soc. 157 (2014), 79–99.

[GM] R. Gupta and M. R. Murty, *A remark on Artin's conjecture*, Invent. Math. 78 (1984), 127–130.

[HW] G. H. Hardy and E. M. Wright, *An Introduction to the Theory of Numbers*, Oxford Univ. Press, 1985.

[Hool] C. Hooley, *On Artin's conjecture*, J. Reine Angew. Math. 225 (1967), 209–220.

[H-B] D. R. Heath-Brown, *Artin's conjecture for primitive roots*, Quart. J. Math. Oxford Ser. (2) 37 (1986), 27–38.

[Kim] S. Kim, *Average reciprocals of the order of a modulo n*, J. Number Theory 166 (2016), 62–75.

[L1] S. Lang, *Undergraduate Analysis*, 2nd ed., Springer, 1997.

[L2] S. Lang, *Algebraic Number Theory*, 2nd ed., Springer, 1994.

[MS] M. R. Murty and S. Srinivasan, *Some remarks on Artin's conjecture*, Canad. Math. Bull. 30 (1987), 80–85.

[Nar] W. Narkiewicz, *Elementary and Analytic Theory of Algebraic Numbers*, 3rd ed., Springer, 2004.

[Rohr] D. E. Rohrlich, *Self-dual Artin representations*, in: Automorphic Representations and L-Functions, D. Prasad et al. (eds.), Tata Inst. Fundam. Res. Stud. Math. 22, Hindustan Book Agency, 2013, 455–499.

Joshua Zelinsky
Department of Mathematics and Statistics
University of Maine
323 Neville Hall
Orono, ME 04469, U.S.A.
E-mail: joshua.zelinsky@maine.edu
zelinsky@gmail.com