An analogue of Artin's conjecture for multiplicative subgroups of the rationals

Francesco Pappalardi & Andrea Susa

Archiv der Mathematik
Archives Mathématiques Archives of Mathematics

ISSN 0003-889X
Volume 101
Number 4

Arch. Math. (2013) 101:319-330
DOI 10.1007/s00013-013-0563-7

Springer

Arch. Math. 101 (2013), 319–330

0003-889X/13/040319-12
published online October 8, 2013
DOI 10.1007/s00013-013-0563-7

Archiv der Mathematik

An analogue of Artin's conjecture for multiplicative subgroups of the rationals

Francesco Pappalardi and Andrea Susa

Abstract. Given $\Gamma \subset \mathbb{Q}^*$ a multiplicative subgroup and $m \in \mathbb{N}^+$, assuming the Generalized Riemann Hypothesis, we determine an asymptotic formula for the number of primes $p \le x$ for which $\mathrm{ind}_p \Gamma = m$, where $\mathrm{ind}_p \Gamma = (p-1)/|\Gamma_p|$ and Γ_p is the reduction of Γ modulo p. This problem is a generalization of some earlier works by Cangelmi–Pappalardi, Lenstra, Moree, Murata, Wagstaff, and probably others. We prove, on GRH, that the primes with this property have a density and, in the case when Γ contains only positive numbers, we give an explicit expression for it in terms of an Euler product. We conclude with some numerical computations.

1. Introduction. Let $\Gamma \subset \mathbb{Q}^*$ be a finitely generated multiplicative subgroup, and let $m \in \mathbb{N}^+$. The *support* of Γ is the (finite) set of primes p for which the p-adic valuation $v_p(g) \neq 0$ for some $g \in \Gamma$. We denote this set by $\mathrm{Supp}\,\Gamma$ and define $\sigma_\Gamma = \prod_{p \in \mathrm{Supp}\,\Gamma} p$. For each prime $p \nmid \sigma_\Gamma$, the set

$$\Gamma_p = \{g (\mathrm{mod} p) : g \in \Gamma\}$$

is well defined. The aim of this paper is to determine, given Γ and m as above, whether there exist infinitely many primes p such that $\mathrm{ind}_p \Gamma = m$. To this purpose we introduce the function:

$$N_\Gamma(x, m) = \#\{p \le x : p \notin \mathrm{Supp}\,\Gamma, \mathrm{ind}_p \Gamma = m\}. \tag{1}$$

So, $N_{\langle a \rangle}(x, 1)$ enumerates the primes p for which $a \in \mathbb{Q}$ is a primitive root modulo p. The famous Artin's conjecture for primitive roots, proved by Hooley in [4] assuming the *Generalized Riemann Hypothesis* (GRH for short), predicts an asymptotic formula for $N_{\langle a \rangle}(x, 1)$ and, in particular, predicts the existence of infinitely many primes p for which a is a primitive root modulo p, as long

as $a \notin \{-1\} \cup \{q^2 : q \in \mathbb{Q}\}$. The work of Hooley was generalized by several authors (including Moree [8], Murata [11], Lenstra [5], Wagstaff [15], and others) who determine, assuming the GRH, an asymptotic formula for $N_{\langle a \rangle}(x, m)$. In particular, Lenstra, Moree, and Stevenhagen, in [6], propose a complete characterization, assuming the GRH, of the pairs (a, m) for which there are no primes $p \nmid a$ with $\mathrm{ind}_p\langle a \rangle = m$. For a complete and updated account, we refer to Moree's Survey [9].

In another direction, the first author and Cangelmi in [1,12] determined, on GRH, an asymptotic formula for $N_\Gamma(x, 1)$, the number of $p \le x$ for which Γ_p contains a primitive root modulo p. The main goal of this paper is to consider $N_\Gamma(x, m)$ in a general context and to propose the following:

Theorem 1. *Let $\Gamma \subset \mathbb{Q}^*$ be a multiplicative subgroup of rank $r \ge 2$, and let $m \in \mathbb{N}$. Assume that the GRH holds for the fields of the form $\mathbb{Q}(\zeta_k, \Gamma^{1/k})$ with $k \in \mathbb{N}$. Then, for any $\epsilon > 0$ and for $m \le x^{\frac{r-1}{(r+1)(4r+2)}-\epsilon}$,*

$$N_\Gamma(x, m) = \left(\rho(\Gamma, m) + O\left(\frac{1}{\varphi(m^{r+1})\log^r x}\right)\right) li(x),$$

where

$$\rho(\Gamma, m) = \sum_{k \ge 1} \frac{\mu(k)}{[\mathbb{Q}(\zeta_{mk}, \Gamma^{1/mk}) : \mathbb{Q}]}. \tag{2}$$

The term $x^{-\epsilon}$ in the above range of uniformity for m can be replaced by a power of $(\log x)^{-1}$, where the power depends on r but it is explicitly computable. Furthermore, the range of uniformity for m in the statement can be removed at the cost of introducing the extra term $x^{(3r+3)/(4r+2)} \log mx$ in the error.

In the special case when $\Gamma \subset \mathbb{Q}^+$, we express the value of $\rho(\Gamma, m)$ as an Euler product. To this purpose, we use the notation

$$\Gamma(k) = \Gamma \cdot \mathbb{Q}^{*k}/\mathbb{Q}^{*k}.$$

An important role is played by the subgroup $\Gamma_2(2^\alpha) \subset \Gamma(2^\alpha)$ consisting of the elements of order dividing 2. Clearly, $\Gamma_2(1)$ is trivial and, if $\alpha > 0$, every element $X \in \Gamma_2(2^\alpha)$ can be written in the form $X = \eta^{2^{\alpha-1}} \cdot \mathbb{Q}^{*2^\alpha}$ for a unique divisor η of σ_Γ. Hence, if $\alpha > 0$, $\Gamma_2(2^\alpha)$ can be identified with the set of integers

$$\{\eta \in \mathbb{N} \colon\ \eta \mid \sigma_\Gamma,\ \eta^{2^{\alpha-1}} \cdot \mathbb{Q}^{*2^\alpha} \in \Gamma(2^\alpha)\}.$$

With the above identification, we denote by $\delta(X) := \delta(\eta)$ where $\delta(\eta)$ is the *field discriminant* of $\mathbb{Q}(\sqrt{\eta})$. Finally, we consider the subgroup $\Gamma'(2^\alpha) \subset \Gamma_2(2^\alpha)$ of those $X \in \Gamma_2(2^\alpha)$ such that $v_2(\delta(X)) \le \alpha$. Hence, if $\alpha > 0$, $\Gamma'(2^\alpha)$ can be identified with the set

$$\{\eta \in \mathbb{N} \colon\ \eta \mid \sigma_\Gamma,\ \eta^{2^{\alpha-1}} \cdot \mathbb{Q}^{*2^\alpha} \in \Gamma(2^\alpha),\ v_2(\delta(\eta)) \le \alpha\}. \tag{3}$$

We prove the following:

Theorem 2. *Let $\Gamma \subset \mathbb{Q}^+ = \{q \in \mathbb{Q}; q > 0\}$ be a multiplicative subgroup of rank $r \ge 2$, and let $m \in \mathbb{N}$. Let*

$$A_{\Gamma,m}=\frac{1}{\varphi(m)|\Gamma(m)|}\times\prod_{\substack{\ell>2\\ \ell\nmid m}}\left(1-\frac{1}{(\ell-1)|\Gamma(\ell)|}\right)\times\prod_{\substack{\ell>2\\ \ell\mid m}}\left(1-\frac{|\Gamma(\ell^{v_\ell(m)})|}{\ell|\Gamma(\ell^{1+v_\ell(m)})|}\right)$$

and

$$B_{\Gamma,k}=\sum_{X\in\Gamma'(2^{v_2(k)})}\prod_{\substack{\ell\mid\delta(X)\\ \ell\nmid k}}\frac{-1}{(\ell-1)|\Gamma(\ell)|-1},$$

where ℓ always denotes a prime number. Then

$$\rho(\Gamma,m)=A_{\Gamma,m}\left(B_{\Gamma,m}-\frac{|\Gamma(2^{v_2(m)})|}{(2,m)|\Gamma(2^{1+v_2(m)})|}B_{\Gamma,2m}\right).$$

Remarks

- It remains to deduce an Euler product for $\rho(\Gamma,m)$ in the case when $\Gamma\not\subset\mathbb{Q}^+$. This task presents more serious technical difficulties and should be addressed in the future.
- A tedious, but routine, computation shows that for $\Gamma=\langle g\rangle$ with $g\in\mathbb{Q}^+$, the formula for $\rho(\Gamma,m)$ coincides with the one due to Wagstaff [15, page 143] or with the one due to Moree [8, Theorem 3].
- Since $|\Gamma(\ell)|=|\Gamma\cdot\mathbb{Q}^{*\ell}/\mathbb{Q}^{*\ell}|=\ell^r$ for all but finitely many primes ℓ (see [1, Section 3] for details), the density $\rho(\Gamma,m)$ is a rational multiple of
$$\prod_{\ell}\left(1-\frac{1}{\ell^r(\ell-1)}\right).$$
- In the special case when $\Gamma=\langle p_1,\dots,p_r\rangle$, where $p_1,\dots,p_r$ are primes in ascending order, we have that $|\Gamma(k)|=k^r$ for all $k\in\mathbb{N}$. Therefore
$$A_{\Gamma,m}=\frac{1}{\varphi(m^{r+1})}\times\prod_{\substack{\ell>2\\ \ell\nmid m}}\left(1-\frac{1}{\ell^r(\ell-1)}\right)\times\prod_{\substack{\ell>2\\ \ell\mid m}}\left(1-\frac{1}{\ell^{r+1}}\right).$$
Furthermore, for $m\in\mathbb{N}$, let
$$C_m=\prod_{\substack{j=1\\ p_j\mid m,p_j>2}}^{r}\left[1+\left(\frac{(-1)^m}{p_i}\right)\right]\times\prod_{\substack{j=1\\ p_j\nmid 2m}}^{r}\left[1-\frac{\left(\frac{(-1)^m}{p_i}\right)}{p_j^r(p_j-1)-1}\right].$$
Then, a calculation shows that
$$\rho(\Gamma,m)=A_{\Gamma,m}\times\begin{cases}1-\frac{1}{2^{r+1}}\,(C_m+C_{2m}) & \text{if } 2\nmid m;\\ \left(\frac{1}{2}C_{\frac{m}{2}}+\left(\frac{1}{2}-\frac{1}{2^{r+1}}\right)C_m\right) & \text{if } 2\|m;\\ \left(1-\frac{(2,p_1)}{2^{r+1}}\right)C_m & \text{if } 4\|m;\\ \left(1-\frac{1}{2^{r+1}}\right)(2,p_1)C_m & \text{if } 8\mid m.\end{cases}\tag{4}$$
- In the classical case when $r=1$, the asymptotic formula in Theorem 1 was proven, on GRH, by L. Murata (see [11, Theorem 1]). Later Fomenko (see [3, Theorem 1(a)]) proved, on GRH, that, if $a\in\mathbb{Q}^*, a\neq\pm1, m\in\mathbb{N}, m\leq\log x$, then

$$N_{\langle a\rangle}(x,m)=\left(\rho(\langle a\rangle,m)+O\left(\frac{\log\log x}{\varphi(m)\log x}\right)\right)\mathrm{li}(x). \tag{5}$$

The techniques of the present paper do not allow any improvement to the uniformity of Fomenko's result.

- If the δ-GRH holds (i.e. the Dedekind zeta function of $\mathbb{Q}(\zeta_k,\Gamma^{1/k})$ has no zeros in the region $\sigma>\delta$) for some $\delta<r/(r+1)$, then the asymptotic formula in Theorem 1 still holds with a larger error term.

2. Notational conventions. Throughout the paper, the letters p and ℓ always denote prime numbers. As usual, we use $\pi(x)$ to denote the number of $p\le x$ and

$$\mathrm{li}(x)=\int_2^x\frac{dt}{\log t}$$

to denote the *logarithmic integral* function.

The letters φ and μ denote respectively the *Euler* and the *Möbius* function. An integer is said to be *squarefree* if it is not divisible by the square of any prime number. If $\eta\in\mathbb{Q}^*$, by $\delta(\eta)$ we denote the *field discriminant* of $\mathbb{Q}(\sqrt{\eta})$. For $\alpha\in\mathbb{Q}^*$ we denote by $v_\ell(\alpha)$ the *ℓ-adic valuation* of α.

For functions F and $G>0$, the notations $F=O(G)$ and $F\ll G$ are equivalent to the assertion that the inequality $|F|\le cG$ holds with some constant $c>0$. In what follows, all constants implied by the symbols O and $\ll$ may depend (when obvious) on the small real parameter ϵ but are absolute otherwise; we write O_λ and $\ll_\lambda$ to indicate that the implied constant depends on a given parameter λ.

3. On the vanishing of the density. In this section we investigate, in the case when $\Gamma\subset\mathbb{Q}^+$, the problem of determining whether

$$\mathcal{N}_{\Gamma,m}=\{p\notin\mathrm{Supp}\,\Gamma,\mathrm{ind}_p\,\Gamma=m\}$$

is finite. If $\Gamma=\langle g\rangle$ with $g\in\mathbb{Q}\backslash\{0,1,-1\}$, this problem has been solved (on GRH) by Lenstra [5, (8.9)–(8.13)] (see also [8]). In fact the following is a special case of Moree's Theorem 4 of [8].

Proposition. *Let $g\in\mathbb{Q}^+\backslash\{1\}$, and write $g=g_0^h$, where $g_0\in\mathbb{Q}^+$ is not the power of any rational number. Then $\rho(\langle g\rangle,m)=0$ if and only if one of the following two conditions is satisfied:*

1. $2\nmid m$, $\delta(g)\mid m$;
2. $v_2(m)>v_2(h)$, $3\mid h$, $3\nmid m$, $\delta(-3g_0)\mid m$.

Furthermore, on GRH, $\mathcal{N}_{\langle g\rangle,m}$ is finite if and only if one of the above two conditions is satisfied.

In the higher rank case, we can generalize the above in the following way:

Proposition 3. *Let $\Gamma\subset\mathbb{Q}^+$ be a non-trivial, finitely generated subgroup, and let $m\in\mathbb{N}$. Then $\rho(\Gamma,m)=0$ when one of the following two conditions is satisfied:*

1. $2 \nmid m$ *and for all* $g \in \Gamma, \delta(g) \mid m$*;*
2. $2 \mid m$, $3 \nmid m$, $\Gamma(3)$ *is trivial, and there exists* $X_0 \in \Gamma'(2^{v_2(m)})$ *such that* 3 *is the only odd prime that divides* $\delta(X_0)$ *and that doesn't divide* m*.*

Furthermore, if m *is odd, the first condition is also necessary in order to have* $\rho(\Gamma, m) = 0$*.*

Proof. Since $A_{\Gamma,m} \neq 0$ for all m and all Γ, the equation $\rho(\Gamma, m) = 0$ is equivalent to

$$B_{\Gamma,m} = \frac{|\Gamma(2^{v_2(m)})|}{(2,m)|\Gamma(2^{1+v_2(m)})|} B_{\Gamma,2m}. \tag{6}$$

If $2 \nmid m$, then the above identity specializes to

$$|\Gamma(2)| = B_{\Gamma,2m} = \sum_{X \in \Gamma'(1)} \prod_{\substack{\ell \mid \delta(X) \\ \ell \nmid 2m}} \frac{-1}{(\ell-1)|\Gamma(\ell)| - 1}.$$

It is clear that if Γ and m satisfy *1.*, then $\Gamma(2) = \Gamma'(2)$ and each factor on the right hand side above equals 1. So (6) is an identity.

On the other hand $|B_{\Gamma,2m}| \leq |\Gamma'(2)| \leq |\Gamma(2)|$. So if (6) is an identity, then $\Gamma'(2) = \Gamma(2)$ and for all $g \in \Gamma$,

$$\prod_{\substack{\ell \mid \delta(g) \\ \ell \nmid 2m}} \frac{-1}{(\ell-1)|\Gamma(\ell)| - 1} = 1.$$

This implies that for all $g \in \Gamma, \delta(g) \mid m$ and the condition in *1.* is satisfied.

Next assume that the condition in *2.* is satisfied. We claim that $B_{\Gamma,m} = B_{\Gamma,2m} = 0$, which implies that (6) is an identity. Observe that

$$\prod_{\substack{\ell \mid \delta(X_0) \\ \ell \nmid 2m}} \frac{-1}{(\ell-1)|\Gamma(\ell)| - 1} = \frac{-1}{2|\Gamma(3)| - 1} = -1.$$

Therefore

$$B_{\Gamma,m} = -\sum_{X \in \Gamma'(2^{v_2(m)})} \prod_{\substack{\ell \mid \delta(X_0 X) \\ \ell \nmid 2m}} \frac{-1}{(\ell-1)|\Gamma(\ell)| - 1} = -B_{\Gamma,m}.$$

By the same argument, we observe that if $X_0 = \eta_0^{2^{v_2(m)-1}} \mathbb{Q}^{*2^{v_2(m)}}$, then $X_0' = \eta_0^{2^{v_2(m)}} \mathbb{Q}^{*2^{v_2(m)+1}} \in \Gamma'(2^{v_2(m)+1})$ also satisfies that 3 is the only odd prime that divides $\delta(X_0')$ and that doesn't divide m. So we deduce that $B_{\Gamma,2m} = 0$, and this concludes the proof. □

Proposition 4. *Assume that* $\Gamma \subset \mathbb{Q}^+$ *and* m *satisfy one of the two conditions of Proposition 3, then* $\mathcal{N}_{\Gamma,m}$ *is finite. Hence, on GRH, if* $2 \nmid m$*,*

$$\mathcal{N}_{\Gamma,m} \text{ finite} \iff \forall g \in \Gamma, \delta(g) \mid m.$$

Proof. Suppose that Γ and m satisfy the first condition in the statement of Proposition 3. Let $p \notin \operatorname{Supp} \Gamma$ and let $g_0 \in \Gamma$ be such that $|\Gamma_p| = |\langle g_0 \rangle| = (p-1)/m$, then $\left(\frac{g_0}{p}\right) = 1$ which implies that $2 \mid m$, a contradiction.

Next suppose that Γ and m satisfy the second condition in the statement of Proposition 3. First note that, if $p \notin \operatorname{Supp}\Gamma$ is a prime such that $|\Gamma_p| = (p-1)/m$, then $p \equiv 2 \bmod 3$ since $3 \nmid m$ and since all elements of Γ are perfect cubes. Furthermore, the hypothesis m even implies that all elements of Γ_p are squares modulo p.

Let $g_0 \in \Gamma$ be such that $X_0 = g_0 \mathbb{Q}^{*2^{v_2(m)}}$. We have that $3 \mid \delta(g_0)$ by hypothesis and that $\delta(-3g_0)$ divides m. Finally

$$\left(\frac{g_0}{p}\right) = \left(\frac{\delta(g_0)}{p}\right) = \left(\frac{-3}{p}\right)\left(\frac{\delta(-3g_0)}{p}\right) = -1,$$

which is a contradiction, and this completes the proof. □

Remarks. Unfortunately, we are unable to show that if $2 \mid m$ and $\rho(\Gamma, m) = 0$, then the second condition in the statement of Proposition 3 is satisfied nor are we able to provide a counterexample for such a property. Possibly the approach due to Lenstra, Moree, and Stevenhagen [6] could provide a complete characterization of the pairs Γ, m with $\rho(\Gamma, m) = 0$ also in the case when Γ contains some negative rational numbers. The techniques of [6] have been adapted to the context of higher rank groups by Moree and Stevenhagen in [10], where the case $m = 1$ is considered.

4. Lemmata. In this section we present some results needed for setting up the proofs. We start by the Chebotarev Density Theorem. The following statement is obtained using the effective version due to Serre [14, Théorème 4].

Lemma 5. (Chebotarev Density Theorem) *Let $\Gamma \subset \mathbb{Q}^*$ be a finitely generated subgroup of rank r and $k \in \mathbb{N}^+$. We denote by $\mathbb{Q}(\zeta_k, \Gamma^{1/k})$ the extension of the cyclotomic field $\mathbb{Q}(\zeta_k)$ obtained by adding the k-th roots of all the elements in Γ. Then the GRH for the Dedekind zeta function of $\mathbb{Q}(\zeta_k, \Gamma^{1/k})$ implies that $\#\{p \le x : p \notin \operatorname{Supp}\Gamma,\ k \mid \operatorname{ind}_p \Gamma\}$ equals*

$$\frac{\operatorname{li}(x)}{\left[\mathbb{Q}(\zeta_k, \Gamma^{1/k}) : \mathbb{Q}\right]} + O\left(\sqrt{x}\log(xk^{r+1}\sigma_\Gamma)\right).$$

The following explicit formula for the degree $\left[\mathbb{Q}(\zeta_k, \Gamma^{1/k}) : \mathbb{Q}\right]$ is proven in [13, Lemma 1 and Corollary 1]:

Lemma 6. *Let $k \ge 1$ be an integer. With the notation above, we have that*

$$\left[\mathbb{Q}(\zeta_k, \Gamma^{1/k}) : \mathbb{Q}(\zeta_k)\right] = |\Gamma(k)|/|\widetilde{\Gamma}(k)|,$$

where

$$\widetilde{\Gamma}(k) = (\Gamma \cap \mathbb{Q}(\zeta_k)^{2^{v_2(k)}}) \cdot \mathbb{Q}^{*2^{v_2(k)}}/\mathbb{Q}^{*2^{v_2(k)}}.$$

Furthermore, in the special case when $\Gamma \subset \mathbb{Q}^+$,

$$\widetilde{\Gamma}(k) = \{\eta \in \mathbb{N} :\ \eta \mid \sigma_\Gamma,\ \eta^{2^{v_2(k)-1}} \mathbb{Q}^{*2^{v_2(k)}} \in \Gamma(2^{v_2(k)}),\ \delta(\eta) \mid k\}.$$

The invariant $\Delta_r(\Gamma)$ of a multiplicative subgroup $\Gamma \subset \mathbb{Q}^*$ with $\operatorname{rank}_{\mathbb{Z}}(\Gamma) = r$ is defined as the greatest common divisor of all the minors of size r of the relation matrix of the group of Γ (see [1, Section 3.1] for some details).

The next result follows immediately from Lemma 6 (see [13, Equation (7)] or [1, Corollary 1]):

Corollary 7. *Let $\Gamma \subset \mathbb{Q}^*$ be a subgroup of $r = \operatorname{rank}_{\mathbb{Z}}(\Gamma)$ and $k \in \mathbb{N}$. Then*

$$2k^r \geq [\mathbb{Q}(\zeta_k, \Gamma^{1/k}) : \mathbb{Q}(\zeta_k)] \geq \frac{(k/2)^r}{\Delta_r(\Gamma)}.$$

Corollary 8. *Let $r = \operatorname{rank}_{\mathbb{Z}}(\Gamma) \geq 2$, and let $P(t)$ denote the product of all primes up to t. Then, for $r \leq t/\log t$, we have the following:*

$$\sum_{k|P(t)} \frac{\mu(k)}{[\mathbb{Q}(\zeta_{mk}, \Gamma^{1/km}) : \mathbb{Q}]} = \rho(\Gamma, m) + O\left(\frac{2^r \Delta_r(\Gamma)}{r\varphi(m^{r+1})t^r}\right). \tag{7}$$

Proof. We apply Corollary 7, and we use the fact that $\varphi(mk) \geq \varphi(m)\varphi(k)$. Hence

$$\frac{1}{[\mathbb{Q}(\zeta_{mk}, \Gamma^{1/km}) : \mathbb{Q}]} \leq \frac{1}{\varphi(m)m^r} \times \frac{2^r \Delta_r(\Gamma)}{\varphi(k)k^r}. \tag{8}$$

Note that

$$\sum_{k|P(t)} \frac{\mu(k)}{[\mathbb{Q}(\zeta_{mk}, \Gamma^{1/mk}) : \mathbb{Q}]} = \rho(\Gamma, m) + O\left(\sum_{k>t} \frac{1}{[\mathbb{Q}(\zeta_{mk}, \Gamma^{1/mk}) : \mathbb{Q}]}\right).$$

The result follows from (8) and from the estimate

$$\sum_{k>t} \frac{1}{\varphi(k^{r+1})} \ll \frac{1}{t^r}\left(\frac{1}{r} + \frac{\log t}{t}\right),$$

which can be derived via partial summation from the classical asymptotic formula

$$\sum_{n \leq t} \frac{n}{\varphi(n)} = \prod_{\ell}\left(1 + \frac{1}{\ell(\ell-1)}\right) t + O(\log t),$$

which can be found for example in [2, Exercises 5.5.3 and 6.5.4]. □

The next lemma is implicit in the work of Matthews [7]:

Lemma 9. *Assume that $\Gamma \subset \mathbb{Q}^*$ is a multiplicative subgroup of rank $r \geq 2$, and assume that $(a_1, \ldots, a_r)$ is a $\mathbb{Z}$-basis of Γ. Let $t \in \mathbb{R}$, $t > 1$. We have the following estimate*

$$\#\{p \notin \operatorname{Supp}\Gamma : |\Gamma_p| \leq t\} \leq 3^r \log(|a_1 \cdots a_r|)\frac{t^{1+1/r}}{\log t}. \tag{9}$$

5. Proof of Theorem 1. Let Γ and m be as above, and set $r = \operatorname{rank}_{\mathbb{Z}}(\Gamma) \geq 2$. Like usual, the proof follows the classical framework of Hooley's [4]. We start with the simple Inclusion–Exclusion Principle:

$$\begin{aligned} N_\Gamma(x, m) &= \#\{p \leq x : p \notin \operatorname{Supp}\Gamma, \operatorname{ind}_p \Gamma = m\} \\ &= \sum_{k \geq 1} \mu(k) \#\{p \leq x : p \notin \operatorname{Supp}\Gamma, mk \mid \operatorname{ind}_p \Gamma\}. \end{aligned}$$

So, for each $t \in [1,x]$, if $P(t)$ denotes the product of all primes up to t, we have

$$U(x;m,t) - E_\Gamma(x;m,t) \le N_\Gamma(x;m) \le U(x;m,t),$$

where

$$U(x;m,t) = \sum_{k|P(t)} \mu(k) \#\left\{p \le x : p \notin \operatorname{Supp}\Gamma, mk | \operatorname{ind}_p \Gamma\right\}$$

and

$$E_\Gamma(x;m,t) = \#\{p \le x : p \notin \operatorname{Supp}\Gamma, \exists \ell > t, \ell m \mid \operatorname{ind}_p \Gamma\}.$$

First, we deal with $U(x;m,t)$. By Lemma 5 (Chebotarev Density Theorem) and Corollary 8, we have:

$$\begin{aligned} U(x;m,t) &= \sum_{k|P(t)} \mu(k) \left(\frac{\operatorname{li}(x)}{[\mathbb{Q}(\zeta_{mk}, \Gamma^{\frac{1}{mk}}) : \mathbb{Q}]} + O\big(\sqrt{x} \log x (mk)^{r+1} \sigma_\Gamma\big)\right) \\ &= \rho(\Gamma,m) \operatorname{li}(x) + O\left(\frac{2^r \Delta_r(\Gamma)}{r\varphi(m^{r+1})t^r} \cdot \frac{x}{\log x}\right) \\ &\quad + O\Big(\sqrt{x} 2^{\pi(t)} \log(x(mP(t))^{r+1}\sigma_\Gamma)\Big). \end{aligned}$$

We choose $t = \log x$ so that $2^{\pi(t)} = x^{O(1/\log\log x)}$. Hence, if $m \le x^{1/(2r+3)}$, then

$$U(x;m,t) = \rho(\Gamma,m)\operatorname{li}(x) + O_\Gamma\left(\frac{x}{\varphi(m^{r+1})(\log x)^{r+1}}\right).$$

In order to estimate $E_\Gamma(x;m,t)$, we define, for any $t \le \xi < \theta \le x$,

$$E_\Gamma(x;m,\xi,\theta) = \#\{p \le x : p \notin \operatorname{Supp}\Gamma, \exists \ell \in (\xi,\theta], \ell m \mid \operatorname{ind}_p \Gamma\}.$$

So

$$E_\Gamma(x;m,t) \le E_\Gamma(x;m,t,\xi) + E_\Gamma(x;m,\xi,x).$$

Applying Lemma 9, we obtain

$$E_\Gamma(x;m,\xi,x) \ll_\Gamma \left(\frac{x}{m\xi}\right)^{1+1/r}.$$

Using Lemma 5 (Chebotarev Density Theorem) and Merten's formula, we deduce:

$$\begin{aligned} E_\Gamma(x,m,t,\xi) &\ll \sum_{\ell \in (t,\xi]} \left(\frac{\operatorname{li}(x)}{[\mathbb{Q}(\zeta_{m\ell}, \Gamma^{1/m\ell}) : \mathbb{Q}]} + \sqrt{x}\log(x(m\ell)^{r+1}\sigma_\Gamma)\right) \\ &\ll_\Gamma \frac{\operatorname{li}(x)}{\varphi(m^{r+1})} \sum_{\ell > t} \frac{1}{\ell^r(\ell-1)} + \sqrt{x} \sum_{\ell < \xi} \log(xm) \\ &\ll_\Gamma \frac{x}{\varphi(m^{r+1})(\log x)^{r+1}} + \sqrt{x}\xi \log(xm). \end{aligned}$$

Finally we choose ξ such that $\left(\frac{x}{\xi}\right)^{1+1/r} = \sqrt{x}\xi$, and we deduce that

$$E_\Gamma(x,m,t,\xi) \ll_\Gamma \frac{x}{\varphi(m^{r+1})(\log x)^{r+1}} + x^{(3r+3)/(4r+2)} \log mx$$

and since $(3r+3)/(4r+2) < 1$ for $r \geq 2$, we deduce the thesis.

6. Proof of Theorem 2. We start by applying Lemma 6:

$$\begin{aligned}\rho(\Gamma,m) &= \sum_{n\geq 1} \frac{\mu(n)}{\varphi(mn)} \frac{|\widetilde{\Gamma}(mn)|}{|\Gamma(mn)|} \\ &= \sum_{\substack{n\geq 1\\(n,2)=1}} \frac{\mu(n)}{\varphi(mn)} \frac{|\widetilde{\Gamma}(mn)|}{|\Gamma(mn)|} + \sum_{\substack{n\geq 1\\(n,2)=1}} \frac{\mu(2n)}{\varphi(2mn)} \frac{|\widetilde{\Gamma}(2mn)|}{|\Gamma(2mn)|},\end{aligned}$$

where

$$\widetilde{\Gamma}(k) = \{\eta \in \mathbb{N} : \eta \mid \sigma_\Gamma, \eta^{2^{v_2(k)-1}} \mathbb{Q}^{*2^{v_2(k)}} \in \Gamma(2^{v_2(k)}),\ \delta(\eta) \mid k\}.$$

So, if we set, for k even,

$$\Gamma_2(k) = \Gamma_2(2^{v_2(k)}) = \left\{\eta \in \mathbb{N} : \eta \mid \sigma_\Gamma, \eta^{2^{v_2(k)-1}} \mathbb{Q}^{*2^{v_2(k)}} \in \Gamma(2^{v_2(k)})\right\}$$

and, for k odd, we set $\Gamma_2(k) = \{1\}$, we deduce that

$$\begin{aligned}\rho(\Gamma,m) &= \sum_{\eta\in\Gamma_2(m)} \sum_{\substack{(n,2)=1\\ \delta(\eta)\mid mn}} \frac{\mu(n)}{\varphi(mn)|\Gamma(mn)|} - \sum_{\eta\in\Gamma_2(2m)} \sum_{\substack{(n,2)=1\\ \delta(\eta)\mid 2mn}} \frac{\mu(n)}{\varphi(2mn)|\Gamma(2mn)|} \\ &= \rho_o - \rho_e.\end{aligned}$$

The condition $\delta(\eta) \mid nm$ is equivalent to $\frac{\delta(\eta)}{\gcd(\delta(\eta),m)} \mid n$. Therefore, if we set

$$\eta_m = \frac{\delta(\eta)}{\gcd(\delta(\eta),m)},$$

then η_m must be odd (i.e. $v_2(\delta(\eta)) \leq v_2(m)$) and ρ_o equals

$$\begin{aligned}&\sum_{\substack{\eta\in\Gamma_2(m)\\ \eta_m \text{ odd}}} \mu(\eta_m) \sum_{\substack{k\in\mathbb{N}\\(k,2\eta_m)=1}} \frac{\mu(k)}{\varphi(km\eta_m)|\Gamma(km\eta_m)|} \\ &= \frac{1}{\varphi(m)|\Gamma(m)|} \sum_{\substack{\eta\in\Gamma_2(m)\\ \eta_m \text{ odd}}} \frac{\mu(\eta_m)}{\varphi(\eta_m)|\Gamma(\eta_m)|} \sum_{\substack{k\in\mathbb{N}\\(k,2\eta_m)=1}} \mu(k) \frac{\varphi((k,m\eta_m))|\Gamma(m\eta_m)|}{\varphi(k)(k,m\eta_m)|\Gamma(km\eta_m)|},\end{aligned}$$

where, for $d = m\eta_m$, we used the identities:

$$\varphi(kd)|\Gamma(kd)| = \varphi(d)|\Gamma(d)| \times \frac{\varphi(k)(k,d)\cdot|\Gamma(kd)|}{\varphi((k,d))\cdot|\Gamma(d)|}$$

and $\varphi(m\eta_m)|\Gamma(m\eta_m)| = \varphi(\eta_m)|\Gamma(\eta_m)| \times \varphi(m)|\Gamma(m)|$. For d fixed, the function $\varphi(k)\frac{(k,d)}{\varphi((k,d))}\frac{|\Gamma(kd)|}{|\Gamma(d)|}$ is multiplicative in k. Hence ρ_o equals

$$\frac{1}{\varphi(m)|\Gamma(m)|}\sum_{\substack{\eta\in\Gamma_2(m)\\ \eta_m \text{ odd}}}\frac{\mu(\eta_m)}{\varphi(\eta_m)|\Gamma(\eta_m)|}\prod_{\substack{\ell>2\\ \ell\nmid\eta_m}}\left(1-\frac{\varphi((\ell,m))|\Gamma(\ell^{v_\ell(m)})|}{(\ell-1)(\ell,m)|\Gamma(\ell^{1+v_\ell(m)})|}\right)$$
$$=\frac{1}{\varphi(m)|\Gamma(m)|}\prod_{\substack{\ell>2\\ \ell\nmid m}}\left(1-\frac{1}{(\ell-1)|\Gamma(\ell)|}\right)\times\prod_{\substack{\ell>2\\ \ell\mid m}}\left(1-\frac{|\Gamma(\ell^{v_\ell(m)})|}{\ell|\Gamma(\ell^{1+v_\ell(m)})|}\right)$$
$$\times\sum_{\substack{\eta\in\Gamma_2(m)\\ \eta_m \text{ odd}}}\frac{\mu(\eta_m)}{\varphi(\eta_m)|\Gamma(\eta_m)|}\prod_{\ell\mid\eta_m}\left(1-\frac{\varphi((\ell,m))|\Gamma(\ell^{v_\ell(m)})|}{(\ell-1)(\ell,m)|\Gamma(\ell^{1+v_\ell(m)})|}\right)^{-1}.$$

A calculation leads to the identity

$$\frac{\mu(\eta_m)}{\varphi(\eta_m)|\Gamma(\eta_m)|}\prod_{\ell\mid\eta_m}\left(1-\frac{\varphi((\ell,m))|\Gamma(\ell^{v_\ell(m)})|}{(\ell-1)(\ell,m)|\Gamma(\ell^{1+v_\ell(m)})|}\right)^{-1}$$
$$=\prod_{\substack{\ell\mid\delta(\eta)\\ \ell\nmid 2m}}\frac{-1}{(\ell-1)|\Gamma(\ell)|-1}.$$

We set

$$A_{\Gamma,m}=\frac{1}{\varphi(m)|\Gamma(m)|}\prod_{\substack{\ell>2\\ \ell\nmid m}}\left(1-\frac{1}{(\ell-1)|\Gamma(\ell)|}\right)\times\prod_{\substack{\ell>2\\ \ell\mid m}}\left(1-\frac{|\Gamma(\ell^{v_\ell(m)})|}{\ell|\Gamma(\ell^{1+v_\ell(m)})|}\right)$$

and

$$B_{\Gamma,m}=\sum_{\substack{\eta\in\Gamma_2(m)\\ \eta_m \text{ odd}}}\prod_{\substack{\ell\mid\delta(\eta)\\ \ell\nmid m}}\frac{-1}{(\ell-1)|\Gamma(\ell)|-1}.$$

Finally observe that, if m is even, $\{\eta\in\Gamma_2(m):\eta_m \text{ is odd}\}=\Gamma'(2^{v_2(m)})$. So the value of $B_{\Gamma,m}$ above is the same as the one in the statement. Furthermore $\rho_o=A_{\Gamma,m}\times B_{\Gamma,m}$, and a similar calculation shows that $\rho_e=A_{\Gamma,2m}\times B_{\Gamma,2m}$. Finally note that

$$\frac{A_{\Gamma,2m}}{A_{\Gamma,m}}=\frac{|\Gamma(2^{v_2(m)})|}{(2,m)|\Gamma(2^{v_2(m)+1})|}.$$

Therefore, subtracting the two expressions for ρ_o and for ρ_e, we obtain

$$\rho=A_{\Gamma,m}\left(B_{\Gamma,m}-\frac{|\Gamma(2^{v_2(m)})|}{(2,m)|\Gamma(2^{v_2(m)+1})|}B_{\Gamma,2m}\right). \tag{10}$$

7. Numerical examples. In this section we compare numerical data. All values, when significant, have been truncated to 7 decimal digits.

The first table compares the values of $\rho(\Gamma_r,m)$ as in (4) (second row) and $N_{\Gamma_r,m}(10^9,m)/\pi(10^9)$ (first row) with $\Gamma_r=\langle 2,\dots,p_r\rangle$, $r\le 7$ (p_i is the $i-th$ prime) and $m=2,\dots,16$.

$m\backslash\Gamma_r$	1	2	3	4	5	6	7
1	0.3739568	0.6975239	0.8568298	0.9313241	0.9667172	0.9837224	0.9919961
	0.3739558	0.6975013	0.8567856	0.9312900	0.9666713	0.9836828	0.9919573
2	0.2804694	0.2051420	0.1146316	0.0601277	0.0306819	0.0154801	0.0077552
	0.2804668	0.2051474	0.1146293	0.0601323	0.0306941	0.0154918	0.0077801
3	0.0664931	0.0394969	0.0159572	0.0057619	0.0019836	0.0006634	0.0002187
	0.0664810	0.0395098	0.0159661	0.0057606	0.0019904	0.0006748	0.0002268
4	0.0467497	0.0205211	0.0065476	0.0017992	0.0004589	0.0001087	0.0000251
	0.0467444	0.0205147	0.0065523	0.0018067	0.0004709	0.0001199	0.0000302
5	0.0189129	0.0069911	0.0014736	0.0003456	0.0000741	0.0000158	3.06×10^{-6}
	0.0188946	0.0069891	0.0014689	0.0003477	0.0000748	0.0000154	3.14×10^{-6}
6	0.0498435	0.0098867	0.0019880	0.0003478	0.0000506	5.54×10^{-5}	8.06×10^{-7}
	0.0498607	0.0098774	0.0019912	0.0003598	0.0000621	1.05×10^{-5}	1.77×10^{-6}
7	0.0089324	0.0023793	0.0004156	0.0000657	9.02×10^{-6}	1.49×10^{-6}	1.76×10^{-7}
	0.0089347	0.0023736	0.0004163	0.0000646	9.58×10^{-6}	1.39×10^{-6}	2.00×10^{-7}
8	0.0350623	0.0059818	0.0008729	0.0001115	1.34×10^{-5}	1.37×10^{-6}	3.34×10^{-7}
	0.0350583	0.0059834	0.0008775	0.0001166	1.49×10^{-5}	1.88×10^{-6}	2.37×10^{-7}
9	0.0073759	0.0014606	0.0001935	0.0000224	2.45×10^{-6}	2.16×10^{-7}	1.96×10^{-8}
	0.0073867	0.0014633	0.0001971	0.0000237	2.73×10^{-6}	3.08×10^{-7}	3.45×10^{-8}
10	0.0141599	0.0020526	0.0004521	0.0000471	4.81×10^{-6}	3.73×10^{-7}	0
	0.0141709	0.0020556	0.0004596	0.0000481	4.91×10^{-6}	4.95×10^{-7}	4.97×10^{-8}
11	0.0033987	0.0005746	0.0000639	6.60×10^{-6}	7.07×10^{-7}	1.96×10^{-8}	$1,96 \times 10^{-8}$
	0.0034024	0.0005764	0.0000643	6.36×10^{-6}	6.00×10^{-7}	5.55×10^{-8}	5.09×10^{-9}
12	0.0083077	0.0024617	0.0002406	1.95×10^{-5}	1.51×10^{-6}	9.83×10^{-8}	0
	0.0083101	0.0024693	0.0002489	2.24×10^{-5}	1.94×10^{-6}	1.64×10^{-7}	1.38×10^{-8}
13	0.0023936	0.0003484	0.0000321	2.79×10^{-6}	3.93×10^{-7}	1.96×10^{-8}	0
	0.0023983	0.0003439	0.0000324	2.71×10^{-6}	2.16×10^{-7}	1.67×10^{-8}	1.30×10^{-9}
14	0.0066952	0.0006957	0.0000547	3.89×10^{-6}	3.34×10^{-7}	0	0
	0.0067010	0.0006981	0.0000557	4.01×10^{-6}	2.98×10^{-7}	2.17×10^{-8}	1.56×10^{-9}
15	0.0033578	0.0003952	0.0000281	1.98×10^{-6}	1.76×10^{-7}	3.93×10^{-8}	0
	0.0033590	0.0003958	0.0000273	2.15×10^{-6}	1.54×10^{-7}	1.06×10^{-8}	0.72×10^{-9}
16	0.0087682	0.0007475	0.0000524	3.34×10^{-6}	1.37×10^{-7}	1.96×10^{-8}	1.96×10^{-8}
	0.0087645	0.0007479	0.0000548	3.64×10^{-6}	2.33×10^{-7}	1.47×10^{-8}	0.92×10^{-9}

Acknowledgements. The author would like to thank the anonymous referee for useful suggestions on how to improve the presentation of the present paper and for suggesting to reference [3]. Regarding [3, Theorem 1(a)] stated in (5), the referee pointed out that making intelligent choices for the parameters ξ_1, ξ_2, and ξ_3 in the proof, one can obtain the following improvement of Fomenko's result:

$$N_{\langle a\rangle}(x,m) = \left(\rho(\langle a\rangle, m) + O\left(\frac{\log\log x}{\varphi(m)\log x} + \frac{1}{\log^A x}\right)\right)\mathrm{li}(x)$$

for any $A > 0$, where the implied constants depends only on a and A. The above holds for any $m \in \mathbb{N}$.

References

[1] L. Cangelmi and F. Pappalardi, On the r-rank Artin Conjecture, II. J. Number Theory **75** (1999), 120–132.

[2] A. C. Cojocaru and R. Murty, An Introduction to Sieve Methods and their Applications, *Cambridge University Press,* New York, 2006.

[3] O. M. Fomenko, Class Numbers of Indefinite Binary Quadratic Forms and the Residual Indices of Integers modulo p, Journal of Mathematical Sciences **122** (2004), 3685–3698.

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

[5] H. W. Lenstra Jr., On Artin's conjecture and Euclid's algorithm in global fields, Invent. Math. **42** (1977), 201–224.

[6] H. W. Lenstra Jr., P. Moree, and P. Stevenhagen, Character sums for primitive root densities, arXiv:1112.4816

[7] C. R. Matthews, Counting points modulo p for some finitely generated subgroups of algebraic groups, Bull. London Math. Soc. **14** (1982), 149–154.

[8] P. Moree, Near-primitive roots, arXiv:1112.5090, Funct. Approx. Comment. Math. **48** (2013), 133–145.

[9] P. Moree, Artin's primitive root conjecture -a survey- Integers **12A** (2012), A13, 100 pp.

[10] P. Moree and P. Stevenhagen, Computing higher rank primitive root densities, arXiv:1203. 4313. To appear in Acta Arith.

[11] L. Murata, A problem analogous to Artin's conjecture for primitive roots and its applications. Arch. Math. (Basel) **57** (1991), 555–565.

[12] F. Pappalardi, The r-rank Artin conjecture, Math. Comp. **66** (1997), 853–868.

[13] F. Pappalardi, Divisibility of reduction in groups of rational numbers, To appear in Math. Comp.

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

[15] S. S. Wagstaff Jr., Pseudoprimes and a generalization of Artin's conjecture. Acta Arith. **41** (1982), 141–150.

Francesco Pappalardi and Andrea Susa
Dipartimento di Matematica, Università Roma Tre,
Largo S. L. Murialdo, 1,
00146 Rome, Italy
e-mail: pappa@mat.uniroma3.it

Andrea Susa
e-mail: andrea.susa@gmail.com

Received: 19 November 2012