MATHEMATICS OF COMPUTATION
Volume 66, Number 218, April 1997, Pages 853–868
S 0025-5718(97)00805-3

ON THE r-RANK ARTIN CONJECTURE

FRANCESCO PAPPALARDI

ABSTRACT. We assume the generalized Riemann hypothesis and prove an asymptotic formula for the number of primes for which $\mathbb{F}_p^*$ can be generated by r given multiplicatively independent numbers. In the case when the r given numbers are primes, we express the density as an Euler product and apply this to a conjecture of Brown–Zassenhaus (J. Number Theory **3** (1971), 306–309). Finally, in some examples, we compare the densities approximated with the natural densities calculated with primes up to $9 \cdot 10^4$.

1. INTRODUCTION

Suppose $a_1, \dots, a_r$ are multiplicatively independent integers none of which is ± 1 or 0 and not all are perfect squares. Let Γ denote the subgroup of $\mathbb{Q}^\times$ generated by $a_1, \dots, a_r$. For all the primes p that do not divide any of $a_1, \dots, a_r$, we consider the reduction of Γ modulo p and denote it by Γ_p. Γ_p can be viewed as a subgroup of $\mathbb{F}_p^*$. We denote by $N_\Gamma(x)$ the number of primes p up to x which do not divide any of the $a_1, \dots, a_r$ and such that

$$\mathbb{F}_p^* = \Gamma_p. \tag{1.1}$$

$N_\Gamma(x)$ measures the number of primes for which $a_1, \dots, a_r$ generate a primitive root $\pmod p$.

In the case $r = 1$, the Artin's Conjecture for primitive roots predicts the probability for a prime p to have a given number a as a primitive root.

For example, if $a = 2$, then Artin Conjecture states that

$$N_{\langle 2\rangle}(x) \sim \prod_{l \text{ prime}} \left(1 - \frac{1}{l(l-1)}\right) \frac{x}{\log x}. \tag{1.2}$$

Hooley [7] has shown that if the generalized Riemann hypothesis holds for the Dedekind zeta function of the fields $\mathbb{Q}(\zeta_l, 2^{1/l})$, with l prime, then the asymptotic formula in (1.2) holds.

The idea of considering "higher rank" analogue to the Artin Conjecture is due to Rajiv Gupta and Maruti Ram Murty who in [6] gave asymptotic formulas for the number of primes p up to x for which r given rational points of an elliptic curve $E/\mathbb{Q}$ generate $\pmod p$ the finite group $E(\mathbb{F}_p)$.

We will prove the following:

Received by the editor April 11, 1995 and, in revised form, January 23, 1996.

1991 *Mathematics Subject Classification.* Primary 11N37; Secondary 11N56.

Key words and phrases. Primitive roots, generalized Riemann hypothesis.

Supported by Human Capital and Mobility Program of the European Community, under contract ERBCHBICT930706.

Theorem 1.1. *Let Γ be as above, set $n_m = [\mathbb{Q}(\zeta_m, a_1^{1/m}, \dots, a_r^{1/m}) : \mathbb{Q}]$ and define*

$$\delta_\Gamma = \sum_{m=1}^{\infty} \frac{\mu(m)}{n_m}. \tag{1.3}$$

The sum in (1.3) converges absolutely and if the generalized Riemann hypothesis holds for the Dedekind zeta function of the fields $\mathbb{Q}(\zeta_m, a_1^{1/m} \dots, a_r^{1/m})$, then

$$N_\Gamma(x) = \delta_\Gamma \operatorname{li}(x) + \mathrm{O}\left(\frac{x \log(a_1 \cdots a_r)}{\log^2 x}\right), \tag{1.4}$$

uniformly with respect to $r \leq \frac{1}{3\log 2} \log x$ and $a_1, \dots, a_r$.

If in addition we suppose that $a_1, \dots, a_r$ are primes, then

$$N_\Gamma(x) = \delta_\Gamma \operatorname{li}(x) + \mathrm{O}\left(\frac{x 4^r \log(x \cdot a_1 \cdots a_r)}{\log^{r+2} x}\right), \tag{1.5}$$

uniformly with respect to $r \leq \frac{1}{4} \frac{\log x}{\log\log x}$ and $a_1, \dots, a_r$.

The value of the density can be expressed as an Euler product. We will do this in the case in which all the $a_1, \dots, a_r$ are primes.

Theorem 1.2. *Let $p_1, \dots, p_r$ be odd primes, $n_m = [\mathbb{Q}(\zeta_m, p_1^{1/m}, \dots, p_r^{1/m}) : \mathbb{Q}]$, $\tilde{n}_m = [\mathbb{Q}(\zeta_m, 2^{1/m}, p_1^{1/m}, \dots, p_r^{1/m}) : \mathbb{Q}]$. Define the r-dimensional incomplete Artin's constant to be:*

$$A_r = \prod_{l \text{ odd prime}} \left(1 - \frac{1}{l^r(l-1)}\right). \tag{1.6}$$

Then

$$\sum_{m=1}^{\infty} \frac{\mu(m)}{n_m} = A_r \left[1 - \frac{1}{2^{r+1}} \left[\prod_{i=1}^{r} \left[1 - \frac{\left(\frac{-1}{p_i}\right)}{p_i^{r+1} - p_i^r - 1}\right] + \prod_{i=1}^{r} \left[1 - \frac{1}{p_i^{r+1} - p_i^r - 1}\right]\right]\right]$$

and

$$\sum_{m=1}^{\infty} \frac{\mu(m)}{\tilde{n}_m} = A_{r+1} \left[1 - \frac{1}{2^{r+2}} \left[\prod_{i=1}^{r} \left[1 - \frac{\left(\frac{-1}{p_i}\right)}{p_i^{r+2} - p_i^{r+1} - 1}\right] + \prod_{i=1}^{r} \left[1 - \frac{1}{p_i^{r+2} - p_i^{r+1} - 1}\right]\right]\right].$$

2. Proof of Theorem 1.1

We first note that

$$n_m \geq [\mathbb{Q}(\zeta_m, a_1^{1/m}) : \mathbb{Q}] \gg \frac{\varphi(m) m}{\log a_1}, \tag{2.1}$$

therefore δ_Γ is a convergent series and thus a well defined number.

The first step of the proof follows the original idea of Hooley who considered the following functions:

$$N_\Gamma(x, y) = \#\left\{p \leq x \;\middle|\; p \nmid a_1 \cdots a_r,\ \forall l,\ l \leq y,\ l \nmid\ [\mathbb{F}_p^* : \Gamma_p]\right\}, \tag{2.2}$$

$$M_\Gamma(x, y, z) = \#\left\{p \leq x \;\middle|\; p \nmid a_1 \cdots a_r,\ \exists l,\ y \leq l \leq z, l\ \middle|[\mathbb{F}_p^* : \Gamma_p]\right\}, \tag{2.3}$$

$$M_\Gamma(x, z) = \#\left\{p \leq x \;\middle|\; p \nmid a_1 \cdots a_r,\ \exists l,\ l \geq z,\ l \middle|[\mathbb{F}_p^* : \Gamma_p]\right\}, \tag{2.4}$$

where y and z are parameters to be chosen later.

Clearly,

$$N_\Gamma(x,y) \geq N_\Gamma(x) \geq N_\Gamma(x,y) - M_\Gamma(x,y,z) - M_\Gamma(x,z). \tag{2.5}$$

By the inclusion–exclusion formula, we find that if μ is the Möbius function, then

$$N_\Gamma(x,y) = \sum\nolimits_m^* \mu(m)\pi_m(x) \tag{2.6}$$

where

$$\pi_m(x) = \# \left\{p \leq x \;\middle|\; p \nmid a_1 \cdots a_r \text{ and } m | [\mathbf{F}_p^*, \Gamma_p] \right\} \tag{2.7}$$

and the upper $*$ means that the sum is extended to all the integers m whose prime divisors are distinct and less than y. Also note that since m is square–free, this forces $m \leq \prod_{q<y} q = e^{\vartheta(y)}$.

It is easy to see that

$$q \mid [\mathbb{F}_p^* : \Gamma_p] \iff p \nmid q \cdot a_1 \cdots a_r \text{ and } p \text{ splits completely in } \mathbb{Q}(\zeta_q, a_1^{1/q}, \ldots, a_r^{1/q}). \tag{2.8}$$

Since a prime splits completely in two distinct fields if and only if it splits completely in their composite, if we let $L_m = \mathbb{Q}(\zeta_m, a_1^{1/m}, \ldots, a_r^{1/m})$, then p ramifies in L_m if and only if $p | m \cdot a_1 \cdots a_r$ and we have that

$$\pi_m(x) = \#\{p \leq x \mid p \text{ is unramified and splits completely in } L_m\}. \tag{2.9}$$

The Chebotarev Density Theorem provides us with an asymptotic formula for π_m. The following is a result due to Lagarias and Odlyzko [8].

Lemma 2.1. *Suppose that L is a Galois extension of $\mathbb{Q}$ with discriminant d_L and degree n_L, and that the generalized Riemann hypothesis holds for the Dedekind zeta function of L; then*

$$\#\{p \leq x \mid p \textit{ is unramified and splits completely in } L\} \tag{2.10}$$

$$= \frac{1}{n_L} \operatorname{li}(x) + \mathrm{O}(x^{1/2} \log(x \cdot d_L^{1/n_L})). \quad \square \tag{2.11}$$

Recall that the Hensel inequality states that

$$\log |d_L| \leq n_L \sum_{q | d_L, q \text{ prime}} \log q. \tag{2.12}$$

Therefore, if we let d_m be the discriminant of L_m and n_m its degree we find that

$$d_m^{1/n_m} \leq \prod_{q | d_m} q \leq m \cdot a_1 \ldots a_r \tag{2.13}$$

and finally

$$\pi_m(x) = \frac{\operatorname{li}(x)}{n_m} + \mathrm{O}\left(x^{1/2} \log(x \cdot m \cdot a_1 \cdots a_r)\right). \tag{2.14}$$

Let us suppose for a moment that $a_1, \dots, a_r$ are prime and put (2.14) into (2.6). We deduce that

$$N_\Gamma(x,y) = \sum\nolimits_m^* \mu(m) \left(\frac{1}{n_m} \operatorname{li}(x) + \mathrm{O}\left(x^{1/2} \log(x \cdot m \cdot a_1 \cdots a_r) \right) \right) \tag{2.15}$$

$$= \sum_{m=1}^{\infty} \frac{\mu(m)}{n_m} \operatorname{li}(x) + \mathrm{O}\left(\sum_{m>y} \frac{2^{\nu(m)}}{m^r \varphi(m)} \operatorname{li}(x) \right) \tag{2.16}$$

$$+ \mathrm{O}\left(e^{\vartheta(y)} x^{1/2} y \log(x \cdot a_1 \cdots a_r) \right) \tag{2.17}$$

$$= \delta_\Gamma \operatorname{li}(x) + \mathrm{O}\left(\frac{1}{y^r} \frac{x}{\log x} + e^{\vartheta(y)} x^{1/2} y \log(x \cdot a_1 \cdots a_r) \right) \tag{2.18}$$

The first identity is a consequence of Corollary 4.2. In the case when $a_1, \dots, a_r$ are not all primes we use (2.1) and we can only deduce that

$$N_\Gamma(x,y) = \delta_\Gamma \operatorname{li}(x) + \mathrm{O}\left(\frac{\log a_1}{y} \frac{x}{\log x} + e^{\vartheta(y)} x^{1/2} y \log(x \cdot a_1 \cdots a_r) \right). \tag{2.19}$$

To deal with the last term of (2.5), we will make use of the following result which is implicit in the work of Matthews [9]:

Lemma 2.2. *Suppose that r is a function of t such that $rt^{-1/r}$ is bounded. Then*

$$\#\{p \mid |\Gamma_p| \le t\} = \mathrm{O}\left(\frac{t^{1+1/r}}{\log t} r 2^r \sum_{i=1}^{r} \log a_i \right) \tag{2.20}$$

where the constants involved in the O *symbol do not depend on t nor r, nor on $\{a_1, \dots, a_r\}$.* □

We note that

$$M_\Gamma(x,z) \le \#\left\{ p \le x \;\middle|\; \exists\, l \ge z,\ l \,\middle|\, \frac{p-1}{|\Gamma_p|} \right\} \tag{2.21}$$

$$\le \#\left\{ p \le x \;\middle|\; |\Gamma_p| \le \frac{x}{z} \right\} \tag{2.22}$$

and applying Lemma 2.2 with $t = x/z$, we find

$$M_\Gamma(x,z) = \mathrm{O}\left((x/z)^{1+1/r} \frac{r 2^r \log(a_1 \cdots a_r)}{\log(x/z)} \right) \tag{2.23}$$

with the condition

$$r \left(\frac{z}{x} \right)^{1/r} = \mathrm{O}(1). \tag{2.24}$$

Finally, for the middle term of (2.5) we have that if $a_1 \dots a_r$ are all prime, then

$$M_\Gamma(x,y,z) \le \#\{\, p \le x \mid \exists\, l,\ y \le l \le z,$$

$$p \text{ is unramified and splits completely in } L_l\} \tag{2.25}$$

$$\le \sum_{y \le l \le z} \left(\frac{1}{l^r(l-1)} \operatorname{li}(x) + \mathrm{O}\left(x^{1/2} \log(x \cdot l \cdot a_1 \cdots a_r) \right) \right), \tag{2.26}$$

since in this case for l odd prime, $n_l = l^r(l-1)$. As

$$\sum_{l \ge y} \frac{1}{l^r(l-1)} \ll \frac{1}{y^r} \tag{2.27}$$

and

$$\sum_{l<z} x^{1/2}\log(x\cdot l\cdot a_1\cdots a_r) \ll x^{1/2}z\log(x\cdot a_1\cdots a_r), \tag{2.28}$$

for $r>1$ we have the estimate:

$$M_\Gamma(x,y,z) \ll \frac{1}{y^r}\frac{x}{\log x} + x^{1/2}z\log(x\cdot a_1\cdots a_r). \tag{2.29}$$

Finally, we put (2.18), (2.23) and (2.29) into (2.5) obtaining:

$$N_\Gamma(x) = \delta_\Gamma \operatorname{li}(x) + \mathrm{O}\left(\frac{1}{y^r}\frac{x}{\log x} + e^{\vartheta(y)}x^{1/2}y\log(x\cdot a_1\cdots a_r)\right) \tag{2.30}$$

$$+\,\mathrm{O}\left((x/z)^{1+1/r}\,\frac{r2^r\log(a_1\cdots a_r)}{\log(x/z)}\right) \tag{2.31}$$

$$+\,\mathrm{O}\left(x^{1/2}z\log(x\cdot a_1\cdots a_r)\right). \tag{2.32}$$

We choose the parameters to optimize the error term setting

$$e^{\vartheta(y)} = \frac{x^{1/2}}{(\log x)^{r+3}}, \quad z = \frac{x^{1/2}}{(\log x)^{r+2}}. \tag{2.33}$$

By the hypothesis made on r, condition (2.24) is verified and we have that $y \lesssim \frac{1}{2}\log x$ and this completes the proof for $r>1$ and $a_1,\dots,a_r$ primes.

In the case when $a_1,\dots,a_r$ are not all primes, we estimate the middle term of (2.5) by

$$M_\Gamma(x,y,z) \ll \frac{\log a_1}{y}\frac{x}{\log x} + x^{\frac{1}{2}}z\log(x\cdot a_1\cdots a_r). \tag{2.34}$$

We use (2.19) instead of (2.18), (2.34) instead of (2.29) and deduce similarly the claim. □

Remark. Let r and $a_1,\dots,a_r$ be fixed. The asymptotic formula in Theorem 1.1 can be proven on the weaker assumption that there exists $a\in\Gamma$ with the property that all the Dedekind zeta functions of the fields $\mathbb{Q}(\zeta_l, a^{1/l})$ (l large prime) have no zeroes in the region

$$\sigma > 1 - \frac{1}{r+1}. \tag{2.35}$$

Indeed, the Generalized Riemann Hypothesis is not crucial in estimating the main term $N_\Gamma(x,y)$ in (2.2) (see Section 3) while the term $M_\Gamma(x,y,z)$ in (2.3) is bounded by

(2.36)
$$\sum_{y\le l\le z} \#\left\{p\le x \;\middle|\; p \text{ is unramified and splits completely in } \mathbb{Q}(\zeta_l, a^{1/l})\right\}.$$

The same technique of Lagarias and Odlyzko (see [8]) with the hypothesis (2.35) on the zeroes of the zeta functions of the fields $\mathbb{Q}(\zeta_l, a^{1/l})$ allows one to prove a version of Lemma 2.1 in which the error term is bounded uniformly by $x^{r/(r+1)}\log xl$ so that (2.36) is

$$\ll \frac{1}{y}\frac{x}{\log x} + zx^{r/(r+1)}\log xz. \tag{2.37}$$

If we choose $z = x^{1/(r+1)}/\log^3 x$, we find that (2.36) is $\mathrm{o}(x/\log x)$.

Finally, the term $M_\Gamma(x,z)$ in (2.4) is bounded by

$$M_\Gamma(x,z,z\log^4 x)+M_\Gamma(x,z\log^4 x). \tag{2.38}$$

The first of these two terms is estimated using the Brun–Titchmarsh Theorem, the Mertens formula and the second term is estimated as in (2.23) applying Lemma 2.2.

3. An unconditional estimate

A. I. Vinogradov in [10] proved the unconditional upper bound

$$N_{\langle 2\rangle}\le\prod_l\left(1-\frac{1}{l^2-l}\right)\frac{x}{\log x}+c\frac{x(\log\log x)^2}{\log^{5/4}x} \tag{3.1}$$

where c is an absolute constant. His method is based on a "non–abelian characters sum decomposition" and the Selberg sieve. In this higher rank context we establish the weaker but more general

Theorem 3.1. *Suppose for simplicity, that r and $a_1,\dots,a_r$ are fixed primes. With the same notation of Theorem 1.1, there exists a constant c_Γ depending only on Γ such that*

$$N_\Gamma(x)\le\delta_\Gamma\frac{x}{\log x}+c_\Gamma\frac{x}{(\log\log x)^r\log x}. \tag{3.2}$$

The proof is based on the unconditional version of the Chebotarev Density Theorem due to Lagarias and Odlyzko (see [8]):

Lemma 3.2 (Chebotarev Density Theorem). *If L is a Galois extension of $\mathbb{Q}$ with discriminant d_L and degree n_L, then there exists an absolute constant c such that for*

$$\sqrt{\log x}\ge c\,n_L^{1/2}\max(\log|d_L|,|d_L|^{1/n_L}), \tag{3.3}$$

one has

$$\#\{p\le x\mid p \text{ splits completely in } L\}=\frac{1}{n_L}\mathrm{li}(x)+\mathrm{O}\left(x\exp(-An_L^{-1/2}\sqrt{\log x})\right), \tag{3.4}$$

where A is a positive constant depending only on c. □

Proof of Theorem 3.1. As in the proof of Theorem 1.1 we have that for a parameter y,

$$N_\Gamma(x)\le N_\Gamma(x,y)=\sum_m{}^{*}\mu(m)\pi_m(x), \tag{3.5}$$

where the sum is the same as in (2.6).

Now, by Lemma 3.2, for

$$n_m\left(\max\left(\log d_m,d_m^{1/n_m}\right)\right)^2\ll\log x, \tag{3.6}$$

we have that

$$\pi_m(x)=\frac{\mathrm{li}(x)}{n_m}+\mathrm{O}\left(x\exp\left(-A\sqrt{\frac{\log x}{n_m}}\right)\right). \tag{3.7}$$

We have already noticed that $n_m\le m^{r+1}$ and $\log d_m\le n_m\log(m\cdot a_1\cdots a_r)$, so the condition in (3.6) is verified if

$$m^{r+1}\left(\max\left(m^{r+1}\log(m\cdot a_1\cdots a_r),m\cdot a_1\cdots a_r\right)\right)^2\ll\log x. \tag{3.8}$$

The last inequality is satisfied for

$$m \ll \frac{\log^{1/(3r+3)} x}{(\log\log x)^{2/(3r+3)}}. \tag{3.9}$$

We finally choose y such that

$$e^{\vartheta(y)} \ll \frac{\log^{1/(3r+3)} x}{(\log\log x)^{2/(3r+3)}} \tag{3.10}$$

and get

$$\begin{aligned} N_\Gamma(x) &\le \delta_\Gamma \frac{x}{\log x} + c_0 \sum_{m>y} \frac{2^{\nu(m)}}{m^r \varphi(m)} \frac{x}{\log x} + c_1 \sum_{m \le e^{\vartheta(y)}} x \exp\left(-A\sqrt{\frac{\log x}{n_m}}\right) \\ &\le \delta_\Gamma \frac{x}{\log x} + c_2 \frac{1}{y^r} \frac{x}{\log x} + c_3 x e^{\vartheta(y)} \exp\left(-A\sqrt{\frac{\log x}{e^{\vartheta(y)(r+1)}}}\right) \quad (3.11) \\ &\le \delta_\Gamma \frac{x}{\log x} + c_4 \frac{x}{\log x (\log\log x)^r}. \quad (3.12) \end{aligned}$$

This completes the proof. □

4. Computation of the densities

In this section we will express the density δ_Γ as an Euler product in the case when $a_1, \dots, a_r$ are all prime.

The first step is to calculate the degrees of L_m over $\mathbb{Q}$.

Theorem 4.1. *Let $p_1, \dots, p_r$ be odd primes, m a square-free integer and let*

$$n_m = [\mathbb{Q}(\zeta_m, p_1^{1/m}, \dots, p_r^{1/m}) : \mathbb{Q}], \tag{4.1}$$

$$\tilde{n}_m = [\mathbb{Q}(\zeta_m, 2^{1/m}, p_1^{1/m}, \dots, p_r^{1/m}) : \mathbb{Q}]. \tag{4.2}$$

Suppose $(m, p_1 \cdots p_r) = p_{i_1} \cdots p_{i_t}$, then $n_m = \frac{\varphi(m) m^r}{2^\alpha}$ and $\tilde{n}_m = \frac{\varphi(m) m^{r+1}}{2^\alpha}$, where

$$\alpha = \begin{cases} 0 & \text{if } m \text{ is odd or } (m, p_1 \cdots p_r) = 1, \\ t & \text{if } m \text{ is even and } p_{i_1} \equiv p_{i_2} \equiv \cdots \equiv p_{i_t} \equiv 1 \pmod 4, \\ t-1 & \text{otherwise.} \end{cases} \tag{4.3}$$

Proof. Fix $m > 1$. We may assume without loss of generality that

$$p_1 \cdots p_t = (p_1 \cdots p_r, m). \tag{4.4}$$

We let

$$K = \mathbb{Q}(\zeta_m), \quad A = K(p_1^{1/m}, \dots, p_t^{1/m}) \tag{4.5}$$

and for any $1 \le i \le r - t$, we let

$$B_i = A(p_{t+1}^{1/m}, \dots, p_{t+i}^{1/m}). \tag{4.6}$$

We have that

$$n_m = [B_{r-t} : \mathbb{Q}] = [B_{r-t} : A][A : K][K : \mathbb{Q}] \tag{4.7}$$

and clearly $[K : \mathbb{Q}] = \varphi(m)$.

The proof is divided into four steps:

Step 1. We claim that

$$[B_{r-t} : A] = m^{r-t}. \tag{4.8}$$

Since the polynomial

$$f(x) = x^m - p_{t+1} \tag{4.9}$$

splits into linear factors in $B_1 = A(p_{t+1}^{1/m})$, we know that $[B_1 : A] = \frac{m}{d}$. Suppose q is a prime with $q|d$, then

$$[A(p_{t+1}^{1/q}) : A] = 1 \text{ or } q. \tag{4.10}$$

If it was q, then we would have that

$$q = [A(p_{t+1}^{1/q}) : A] \Big| [B_1 : A] = \frac{m}{d} , \tag{4.11}$$

which is a contradiction since m is square–free. Therefore $p_{t+1}^{1/q} \in A$, which implies that p_{t+1} ramifies in $A/\mathbb{Q}$. Now, from Kummer's theory, we know that the only primes that ramify in A are $p_1, \ldots , p_t$ and those that divide m, and since $(p_{t+1}, m) = 1$, we conclude that $d = 1$.

By induction, we have that

$$[B_{r-t} : A] = [B_{r-t} : B_{r-t-1}][B_{r-t-1} : A] = [B_{r-t} : B_{r-t-1}]m^{r-t-1}, \tag{4.12}$$

so again,

$$[B_{r-t} : B_{r-t-1}] = \frac{m}{d} \tag{4.13}$$

and since $(p_r, m) = 1$, we conclude that $d = 1$. Hence $[B_{r-t} : A] = m^{r-t}$.

Step 2. If we let

$$A_i = K(p_1^{1/m}, \ldots , p_i^{1/m}), \tag{4.14}$$

then $A_{i+1} = A_i(p_{i+1}^{1/m})$, and for the same reason as in Step 1,

$$[A_{i+1} : A_i] = \frac{m}{e}. \tag{4.15}$$

We claim that $e = 1$ or 2. Let $q|e$ be a prime divisor and consider $A_i(p_{i+1}^{1/q})$. Since m is square–free, we have that $p_{i+1}^{1/q} \in A_i$. If $p_{i+1}^{1/q} \in K$, then we would have a cyclic extension of prime degree (over $\mathbb{Q}$)

$$\mathbb{Q}(p_{i+1}^{1/q}) \subset K \tag{4.16}$$

and this is only possible when $q = 2$. Therefore we may assume that $p_{i+1}^{1/q} \notin K$, having extensions:

$$K \subseteq K(p_{i+1}^{1/q}) \subseteq A_i. \tag{4.17}$$

Note that $\mathrm{Gal}(A_i/K)$ is the direct product of cyclic groups and a general subgroup of order q has as fixed field

$$K((p_{s_1} \cdots p_{s_k})^{1/q}), \tag{4.18}$$

with $1 \leq s_1 \leq \cdots \leq s_k \leq i - 1$. Therefore

$$K(p_{i+1}^{1/q}) = K((p_{s_1} \cdots p_{s_k})^{1/q}) \tag{4.19}$$

and from Lemma 3 on page 87 of [1], we have that there exists $0 \leq i \leq q-1$ such that

$$\left(\frac{p_{i+1}}{(p_{s_1}\cdots p_{s_k})^i}\right)^{1/q} \in K, \tag{4.20}$$

and again this implies that $q = 2$.

Therefore, if m is odd, $[A_{i+1} : A_i] = m$ for every i, and thus $[A_t : K] = m^t$.

From the Theory of Cyclotomic Fields, we know that the general quadratic subfield of K is

$$\mathbb{Q}(\sqrt{(\tfrac{-1}{D})D}), \tag{4.21}$$

where D is a positive divisor of m. We gather that if $p_i \equiv 1 \pmod 4$, $1 \leq i \leq t$, then $\left(\frac{-1}{p_i}\right) = 1$, hence $\sqrt{p_i} \in K$.

Step 3. If $p_1 \equiv p_2 \equiv \cdots \equiv p_t \equiv 1 \pmod 4$, then let ζ_m be a primitive m–th root of unity. $\mathrm{Gal}(A_1/K)$ is generated by

$$\sigma : p_1^{1/m} \mapsto \zeta_m^2 p_1^{1/m}. \tag{4.22}$$

Note that $\sigma(\sqrt{p_1}) = (\sigma(p_1^{1/m}))^{m/2} = (\zeta_m^2)^{m/2} p_1^{(1/m)(m/2)} = \sqrt{p_1}$ and hence,

$$|\,\mathrm{Gal}(A_1/K)| = [A_1 : K] = \frac{m}{2}. \tag{4.23}$$

Similarly $\mathrm{Gal}(A_{i+1}/A_i)$ is generated by

$$\sigma : p_{i+1}^{1/m} \mapsto \zeta_m^2 p_{i+1}^{1/m}, \tag{4.24}$$

therefore $[A_{i+1} : A_i] = \frac{m}{2}$ and $[A : K] = \frac{m^t}{2^t}$.

Step 4. If there exists $1 \leq i \leq t$ such that $p_i \equiv 3 \pmod 4$, then we can suppose without loss of generality that $p_1 \equiv 3 \pmod 4$.

Let us consider $A_1 = K(p_1^{1/m})$. We have that

$$[A_1 : K] = m. \tag{4.25}$$

Indeed, if not, we would have $K(\sqrt{p_1}) = K$, but again this happens only if $p_1 \equiv 1 \pmod 4$, which is a contradiction. Now consider $i > 1$, and $A_i = A_{i-1}(p_i^{1/m})$. We claim that

$$[A_i : A_{i-1}] = \frac{m}{2}. \tag{4.26}$$

Indeed either $p_i \equiv 1 \pmod 4$ or $p_i \equiv 3 \pmod 4$; in the first case $\sqrt{p_i} \in K$, in the second case $\sqrt{p_1 p_i} \in K$. In any case, $\mathrm{Gal}(A_i/A_{i-1})$ is generated by

$$\sigma : p_i^{1/m} \mapsto \zeta_m^2 p_i^{1/m}. \tag{4.27}$$

Finally we have that

$$[A_i : A_{i-1}] = \frac{m}{2} \tag{4.28}$$

and

$$[A : K] = \frac{m^t}{2^{t-1}}. \tag{4.29}$$

This completes the proof of the first part of the theorem.

For the second part of the statement we note that

$$\tilde{n}_m = [B_{r-t}(2^{1/m}) : B_{r-t}]n_m = n_m m \tag{4.30}$$

using the same argument of Step 3 and noticing that for m square-free, $\sqrt{2} \notin K$.

This concludes the proof of the theorem. □

Remark. A similar result as in Theorem 4.1 is due to P. D. T. A. Elliott (see [3] and [4]).

The formulas of his Lemma 4 and Lemma 5 do not seem correct in general. Indeed consider the field $K = \mathbb{Q}(\zeta_{42}, 3^{1/42}, 7^{1/42})$. From Theorem 4.1 we know that $[K : \mathbb{Q}] = \varphi(42) \cdot 42^2/2$. This can be verified directly by noticing that, since $\sqrt{7} \in \mathbb{Q}(\zeta_{42}, \sqrt{3})$: $K = \mathbb{Q}(\zeta_{42}, \sqrt{3}, 3^{1/3}, 7^{1/7}, 3^{1/7}, 7^{1/3})$. On the other hand Lemma 5 of Elliott's result would imply that $[K : \mathbb{Q}] = \varphi(42) \cdot 42^2$. Therefore in this case his formula does not hold.

The next statement has already been used during the proof of Theorem 1.1.

Corollary 4.2. *With the same notation as in Theorem 4.1, we have*

$$n_m \geq m^r \varphi(m)/2^{\min(r, \nu(m)-1)} \tag{4.31}$$

(*where $\nu(m)$ is the number of distinct prime divisors of m*). *Furthermore such a lower bound is the best possible.* □

Remark. If we drop the condition that $p_1, \dots, p_r$ are primes in Theorem 4.1, then the estimate of Corollary 4.2 does not hold anymore. Indeed if $K = \mathbb{Q}(\zeta_{21}, 5^{1/21}, 40^{1/21})$, then $[K : \mathbb{Q}] = \varphi(21) \cdot \frac{21^2}{3}$ giving a counterexample to (4.31).

We are now ready to express the density as an Euler product. The case $r = 1$ has been dealt with by C. Hooley in [7]. We report it here for completeness:

Lemma 4.3. *Let p be a prime, $n_m = [\mathbb{Q}(\zeta_m, p^{1/m}) : \mathbb{Q}]$ and let*

$$A = \prod_{l \ prime} \left(1 - \frac{1}{l(l-1)}\right) \tag{4.32}$$

be Artin's constant, then we have:

$$\sum_{m=1}^{\infty} \frac{\mu(m)}{n_m} = \begin{cases} A & \text{if } p \not\equiv 1 \pmod{4}, \\ A\left(1 + \frac{1}{p^2-p-1}\right) & \text{if } p \equiv 1 \pmod{4}. \end{cases} \tag{4.33}$$

Proof. If $p \not\equiv 1 \pmod 4$, then $n_m = m\varphi(m)$ for every m and the result follows from the definition of Artin's constant. We can therefore assume that $p \equiv 1 \pmod 4$, having:

$$\sum_{m=1}^{\infty} \frac{\mu(m)}{n_m} = \Sigma_o + \Sigma_e, \tag{4.34}$$

where Σ_o is the sum extended to the odd values of m and Σ_e to the even values. Clearly $\Sigma_o = 2A$ and $\Sigma_e = -\frac{1}{2}\Sigma'_e$, with

$$\Sigma'_e = \sum_{\substack{m=1\\(m,2p)=1}}^{\infty} \frac{\mu(m)}{m\varphi(m)} + 2\sum_{\substack{m=1\\p|m,m \text{ odd}}}^{\infty} \frac{\mu(m)}{m\varphi(m)} \tag{4.35}$$

$$= 2A + \frac{-1}{p(p-1)} \sum_{\substack{m=1\\(m,2p)=1}} \frac{\mu(m)}{m\varphi(m)} \tag{4.36}$$

$$= 2A + \frac{-1}{p(p-1)} \frac{2A}{\left(1-\frac{1}{p(p-1)}\right)} = 2A - \frac{2A}{p^2-p-1}.$$

Finally $\Sigma_o + \Sigma_e = A\left(1+\frac{1}{p^2-p-1}\right)$. □

The general case is similar:

Proof of Theorem 1.2. As in the case $r = 1$, note that if m is odd, then $n_m = m^r\varphi(m)$; thus we can write:

$$\sum_{m=1}^{\infty} \frac{\mu(m)}{n_m} = A(r) + \Sigma \tag{4.37}$$

where Σ is the sum extended to the even values of m. Let $P = p_1 \cdots p_r$ and $\tilde{P} = \prod_{i=1,\ p_i\equiv 1(4)}^{r} p_i$, if m is an odd positive integer and $Q = (m, P)$, then by Theorem 4.1, we have

$$n_{2m} = \begin{cases} 2^r \frac{m^r\varphi(m)}{2^{\nu(Q)}} & \text{if } Q|\tilde{P}, \\ 2^r \frac{m^r\varphi(m)}{2^{\nu(Q)-1}} & \text{otherwise.} \end{cases} \tag{4.38}$$

For any $Q|P$, let $S(Q) = \{m \in \mathbf{N}|\ (m,P) = Q\}$. We have that $\mathbf{N} = \bigcup_{Q|P} S(Q)$, and the union is disjoint. Therefore,

$$\Sigma = \sum_{Q|P} \sum_{m\in S(Q)} \frac{\mu(2m)}{n_{2m}}. \tag{4.39}$$

Now divide the set of divisors of P into two sets; the divisors of $\tilde{P}$, and its complement. It follows that

$$\Sigma = \sum_{Q|\tilde{P}} \sum_{m\in S(Q)} \frac{\mu(2m)2^{\nu(Q)}}{2^r m^r\varphi(m)} + \sum_{\substack{Q|P\\Q\nmid\tilde{P}}} \sum_{m\in S(Q)} \frac{\mu(2m)2^{\nu(Q)-1}}{2^r m^r\varphi(m)} \tag{4.40}$$

$$= \frac{1}{2^{r+1}} \left\{ \sum_{Q|\tilde{P}} 2^{\nu(Q)} \sum_{m\in S(Q)} \frac{\mu(2m)}{m^r\varphi(m)} + \sum_{Q|P} 2^{\nu(Q)} \sum_{m\in S(Q)} \frac{\mu(2m)}{m^r\varphi(m)} \right\}. \tag{4.41}$$

The sum over $m \in S(Q)$ is easy to evaluate,

$$\sum_{m\in S(Q)} \frac{\mu(2m)}{m^r\varphi(m)} = -\frac{(-1)^{\nu(Q)}}{Q^r\varphi(Q)} \sum_{(m,2P)=1} \frac{\mu(m)}{m^r\varphi(m)} \tag{4.42}$$

$$= -\frac{(-1)^{\nu(Q)}}{Q^r\varphi(Q)} A(r) \prod_{i=1}^{r} \left(1 - \frac{1}{\alpha_i+1}\right)^{-1}, \tag{4.43}$$

where for clarity we have set $\alpha_i = p_i^r(p_i - 1) - 1$.

Substituting we get:

$$\Sigma = \frac{-A(r)}{2^{r+1}} \prod_{i=1}^{r}\left(1 - \frac{1}{\alpha_i + 1}\right)^{-1} \left(\sum_{Q \mid \tilde{P}} \frac{(-2)^{\nu(Q)}}{Q^r \varphi(Q)} + \sum_{Q \mid P} \frac{(-2)^{\nu(Q)}}{Q^r \varphi(Q)} \right) \tag{4.44}$$

$$= \frac{-A(r)}{2^{r+1}} \prod_{i=1}^{r}\left(\frac{\alpha_i + 1}{\alpha_i}\right) \left(\prod_{\substack{i=1 \\ p_i \equiv 1(4)}}^{r} \left(1 - \frac{2}{\alpha_i + 1}\right) + \prod_{i=1}^{r}\left(1 - \frac{2}{\alpha_i + 1}\right) \right) \tag{4.45}$$

$$= \frac{-A(r)}{2^{r+1}} \left(\prod_{\substack{i=1 \\ p_i \equiv 1(4)}}^{r} \left(1 - \frac{1}{\alpha_i}\right) \prod_{\substack{i=1 \\ p_i \equiv 3(4)}}^{r} \left(1 + \frac{1}{\alpha_i}\right) + \prod_{i=1}^{r}\left(1 - \frac{1}{\alpha_i}\right) \right). \tag{4.46}$$

The claim is therefore deduced.

The second part of the statement is proved in the same manner, just by noticing that $\tilde{n}_m = n_m m$. □

The next statement is important for the application.

Corollary 4.4. *Let $\{q_i\}_{i>1}$ be an infinite sequence of primes and let δ_r be the density of the set of primes p for which $\mathbb{F}_p^*$ is generated by $q_1, \dots, q_r$, then*

$$\delta_r = 1 + \mathrm{O}\left(\frac{1}{2^r}\right). \quad \square \tag{4.47}$$

Proof. Let A_r be defined as in the statement of Theorem 4.1. First we note that for $r > 1$,

$$A_r < 1 - \frac{1}{2 \cdot 3^r}. \tag{4.48}$$

It is also clear that

$$A_r > \prod_{l>2}\left(1 - \frac{1}{l^r}\right) > \frac{1}{\zeta(r)} = 1 + \mathrm{O}\left(\frac{1}{2^r}\right). \tag{4.49}$$

Finally it is enough to notice that

$$\prod_{i=1}^{r}\left[1 - \frac{\left(\frac{-1}{p_i}\right)}{p_i^{r+2} - p_i^{r+1} - 1}\right] + \prod_{i=1}^{r}\left[1 - \frac{1}{p_i^{r+2} - p_i^{r+1} - 1}\right] \tag{4.50}$$

is bounded as $r \to \infty$ to deduce the claim. □

It is conceivable that for any *infinite sequence of multiplicatively independent integers* (that is a sequence of integers such that $a_i < a_{i+1}$ and for any r, $a_1, \dots, a_r$ are multiplicatively independent) the same result as Corollary 4.4 holds.

5. Application to the conjecture of Brown–Zassenhaus

Let q_i be the i^{th} prime number. For a given prime p, the κ function of Brown–Zassenhaus is defined as follows:

$$\kappa(p) = \min\left\{i \left|\langle q_1, \dots, q_i\right| \pmod p\rangle = \mathbb{F}_p^*\right\}, \tag{5.1}$$

(i.e. $k(p)$ is the least index i such that the first i primes generate a primitive root (mod p)). The conjecture of Brown–Zassenhaus [2] states that:

The probability that $\kappa(p) \le [\log p]$ is almost (but not equal to) one.

To be precise, let $N(x)$ be the number of primes $p \le x$ with $\kappa(p) > [\log p]$. Then the Brown–Zassenhaus conjecture is the two assertions:

(i) $N(x) = o(\pi(x))$,
(ii) $N(x)$ is unbounded.

Statement (ii) is a consequence of the work of Graham and Ringrose [5]. Indeed they proved that the least quadratic non residue is greater than $c \log p \log\log\log p$ for infinitely many primes p. Clearly, this implies (ii).

The results of the preceding sections imply the following:

Proposition 5.1. *With the same notation as above,*

(1) *For every fixed r, there exists a set of primes p with density greater than or equal to $1 - \delta_r$ for which $\kappa(p) > r$;*

(2) *If the GRH holds, then $\kappa(p) \le r$ for a set of primes p of density δ_r;*

(3) *Suppose the GRH holds.*

There exists a positive absolute constant A such that, for all primes $p \le x$ with at most

$$\mathrm{O}\left(\pi(x) \exp\left(-A \log x / \log\log x\right)\right) \tag{5.2}$$

exceptions, we have that

$$\kappa(p) \le \left[\frac{\log p}{4 \log\log p}\right]. \tag{5.3}$$

More generally, there is a positive absolute constant B such that for every divergent function $y = y(x) \le \frac{\log x}{4 \log\log x}$ and for all primes $p \le x$ with at most $\mathrm{O}\left(\pi(x) B^{-y(x)}\right)$ exceptions, we have that

$$\kappa(p) \le [y(p)]. \tag{5.4}$$

Proof. (1) is a direct consequence of Theorem 3.1 while (2) is a direct consequence of Theorem 1.1.

For (3) we apply Corollary 4.4 and Theorem 1.1 with $\Gamma = \langle q_1, \dots, q_{[y]}\rangle$ and get that for $y \le \log x / 4 \log\log x$,

$$N_\Gamma(x) = \pi(x) + \mathrm{O}\left(\frac{1}{2^y} \frac{x}{\log x}\right) + \mathrm{O}\left(\frac{x 4^y (\log x + y \log y)}{\log^{y+2} x}\right). \tag{5.5}$$

The first error term is dominant.

Now we may suppose $p \ge x^{1/2}$, having that $y(p) \gg y(x)$. Finally the number of primes p, $x^{1/2} \le p \le x$ with $\kappa(p) \ge [y(p)] \gg y(x)$, is bounded by

$$\pi(x) - N_\Gamma(x) \ll \frac{x}{\log x} A^{-y(x)}, \tag{5.6}$$

and this completes the proof. □

6. Computation

In this last section we will present three tables comparing the densities δ_Γ with the number $\tilde{\delta}_\Gamma$ defined as

$$\tilde{\delta}_\Gamma = \frac{\#\{q \mid \pi(q) \le 9 \cdot 10^4, \mathbb{F}_q^* = \Gamma_q\}}{9 \cdot 10^4}. \tag{6.1}$$

The computation was performed using Maple V with a Work Station at the University of Paris-Sud.

Table 1

Γ	δ_Γ	$\tilde{\delta}_\Gamma$
$\langle 2 \rangle$	0.37396	0.37368
$\langle 2,3 \rangle$	0.69750	0.69779
$\langle 2,3,5 \rangle$	0.85679	0.85794
$\langle 2,3,5,7 \rangle$	0.93129	0.93253
$\langle 2,3,5,7,11 \rangle$	0.96667	0.96798
$\langle 2,3,5,7,11,13 \rangle$	0.98368	0.98484

The next table considers subgroups generated by odd primes.

Table 2

Γ	δ_Γ	$\tilde{\delta}_\Gamma$
$\langle 3 \rangle$	0.37396	0.37403
$\langle 3,5 \rangle$	0.69985	0.70069
$\langle 3,5,7 \rangle$	0.85678	0.85777
$\langle 3,5,7,11 \rangle$	0.93129	0.93242
$\langle 3,5,7,11,13 \rangle$	0.96667	0.96779
$\langle 3,5,7,11,13,17 \rangle$	0.98368	0.98464

Table 3 needs an explanation: The first line corresponding to the slot i, j contains the value of $\delta_{\langle i,j \rangle}$ while the second line contains $\tilde{\delta}_{\langle i,j \rangle}$.

TABLE 3

	19	17	13	11	7	5	3
2	.69750 .69923	.69755 .69863	.69762 .69812	.69750 .69940	.69750 .69803	.69985 .70096	.69750 .69779
3	.69750 .69857	.69755 .69852	.69762 .69810	.69749 .69796	.69745 .69846	.69985 .70069	
5	.69985 .70146	.69990 .70104	.69996 .70031	.69985 .70066	.69985 .70009		
7	.69750 .69887	.69755 .69886	.69762 .69888	.69750 .69882			
11	.69750 .69938	.69755 .69932	.69762 .69936				
13	.69762 .70011	.69767 .69740					
17	.69755 .69829						

While performing the computation we discovered the following new examples of primes for which the κ function has value larger than 12. These examples are not in the paper of Brown–Zassenhaus [2].

TABLE 4

p	$\kappa(p)$	$\log p$
366791	14	12.81
514751	14	13.15
880871	13	13.69
1083289	13	13.90
1139519	13	13.95
1579751	13	14.27
1884791	13	14.45

The first five primes are interesting since they satisfy

$$\kappa(p) \geq [\log p]. \tag{6.2}$$

Together with those in [2], they provide a complete list of the primes $p \leq 2 \cdot 10^6$ with $\kappa(p) \geq 13$.

ACKNOWLEDGMENTS

I would like to thank Professor Ram Murty for his suggestions and Professor Hershy Kisilevsky for a number of interesting observations.

I thank Professor Carl Pomerance for his help during the redaction of the final version of this paper.

References

1. B. J. Birch, *Cyclotomic fields and Kummer extensions*, Algebraic Number Theory, (J. W. S. Cassels and A. Fröhlich, eds.), Academic Press, 1967, pp. 85–93. MR **36:**25288
2. H. Brown and H. Zassenhaus, *Some empirical observations on primitive roots*, J. Number Theory **3**(1971), 306–309. MR **44:**5270
3. P. D. T. A. Elliott, *A problem of Ërdos concerning power residue sums*, Acta Arith. **13** (1967), 131–149. MR **36:**3741
4. ———, *Corrigendum to the paper "A problem of Ërdos concerning power residue sums"*, Acta Arith. **14** (1968). MR **37:**4031
5. S. W. Graham and C. J. Ringrose, *Lower bounds for the least quadratic non–residues*, Analytic Number Theory (Allerton Park, IL, 1989), 269–309, Progr. Math, 85, Birkhauser, Boston, 1990. MR **92d:**11108
6. R. Gupta and M. R. Murty, *Primitive points on elliptic curves*, Compositio Math. **58**(1986), 13–44. MR **87h:**11050
7. C. Hooley, *On Artin's conjectures*, J. Reine Angew. Math. **225**(1967), 209–220. MR **34:**7445
8. J. C. Lagarias and A. M. Odlyzko, *Effective versions of the Chebotarev Density Theorem*, Algebraic Number Fields (Ed. A. Fröhlich), Academic Press, New York, 1977, pp. 409–464. MR **56:**5506
9. C. R. Matthews, *Counting points modulo p for some finitely generated subgroups of algebraic groups*, Bull. London Math. Soc. **14**(1982), 149–154. MR **83c:**10067
10. A. I. Vinogradov, *Artin L–series and his conjectures*, Proc. Steklov Inst. Math. **112** (1971), 124–142. MR **49:**4977

Dipartimento di Matematica, Università degli Studi di Roma Tre, Via C. Segre, 2, 00146 Rome, Italy
E-mail address: pappa@matrm3.mat.uniroma3.it