Pure and Applied Mathematics Quarterly
Volume 4, Number 4
(*Special Issue: In honor of
Jean-Pierre Serre, Part 1 of 2*)
1279—1290, 2008

On a Generalization of Artin's Conjecture

Cameron Franc * and **M. Ram Murty**†

in honour of J.-P. Serre on his 80th birthday

§1. Introduction

A primitive root mod p is a generator of $(\mathbb{Z}/p\mathbb{Z})^*$. Gauss was the first to introduce the idea of a primitive root in his *Disquisitiones Arithmeticae*. They were first used to answer questions about the decimal expansion of fractions $1/p$, and have fascinated mathematicians ever since. In 1927, Artin conjectured that every non-square integer a different from 1 or -1 is a primitive root for infinitely many primes p. He also provided a heuristic argument for the conjectured density of such primes [1]. Computations performed by Lehmer showed that this density was incorrect for some values of a, so that a correction factor was required. In 1967, Hooley assumed the generalised Riemann hypothesis (see below) and was able to prove Artin's conjecture with a modified density. Many other important results surrounding Artin's conjecture have been proven (see [6], for example). The unconditional conjecture remains open as of 2006.

Some of the progress on the classical Artin primitive root conjecture was inspired by elliptic analogues of the conjecture formulated by Lang and Trotter [11] and J.-P. Serre [16]. These analogues naturally led the second author to consider the higher rank case of the classical primitive root conjecture and one could say that this was a turning point in the subject (see [6], [13] and [14]). The advances in the theory also led to other applications, most notably to the study of Euclidean rings (see [8]). From this perspective, it is often useful to consider different generalizations of a difficult problem, in the hope that its study will perhaps shed new light on the classical case.

Received August 28, 2006.
*Research partially supported by an NSERC Undergraduate Student Research Award.
†Research partially supported by an NSERC Research grant.

During the summer of 2004, Solomon Golomb related a "natural" generalisation of Artin's conjecture to one of the authors [4].

> *Conjecture.* For every squarefree integer $a > 1$, and for every positive integer r, there are infinitely many primes $p \equiv 1 \pmod r$ such that the order of a in $(\mathbb{Z}/p\mathbb{Z})^*$ is $(p-1)/r$. Moreover, the density of such primes p is asymptotic to a constant (expressible in terms of a and r) times the corresponding asymptotic density for the case $r = 1$ (Artin's conjecture).

His conjecture arose in connection with the divisibility of polynomials over $GF(q)$ with a restricted number of terms [5]. Golomb performed extensive computations for various r when $a = 2$. They seemed to support his conjecture and, in particular, indicated a density of

$$\frac{A(2)}{r^2}\left(\frac{r^2-1}{r^2-r-1}\right)$$

for odd prime values of r, where $A(2)$ is Artin's constant. In this paper we will assume the generalised Riemann hypothesis and follow Hooley's method in order to prove results towards a resolution of Golomb's conjecture.

We must introduce some notation before we can begin the analysis. Throughout the paper, a will denote a fixed positive integer that is not a p-th power for any prime p. The symbol r will also represent a fixed positive integer, and k will usually be reserved for positive squarefree integers. A primitive n-th root of unity will always be denoted by ζ_n. The object of inquiry is the function $\mathsf{N}_{\mathsf{a},\mathsf{r}}(x)$, which counts the primes $p \le x$ satisfying $p \equiv 1 \pmod r$ and such that a has multiplicative order $(p-1)/r$ modulo p. Our goal is to use the generalised Riemann hypothesis to find an asymptotic formula for $\mathsf{N}_{\mathsf{a},\mathsf{r}}(x)$.

For our purpose, it is necessary to reformulate the condition that a has order $(p-1)/r$. A necessary and sufficient condition for a to have order $(p-1)/r$ is that $a^{(p-1)/r} \equiv 1 \pmod p$ and whenever $p \equiv 1 \pmod{rq}$ for a prime q, then $a^{(p-1)/(rq)} \not\equiv 1 \pmod p$. If we let $R(p,k)$ correspond to the simultaneous conditions

$$\begin{aligned} &p \equiv 1 \pmod{rk} \\ &a^{(p-1)/(rk)} \equiv 1 \pmod p \end{aligned}$$

then a has order $(p-1)/r$ if and only if $R(p,1)$ holds, but $R(p,q)$ does not for every prime q. We adopt the formalism introduced by Hooley so that we can restate this once again in the language of algebraic number theory.

Let L_r denote the Galois number field $\mathbb{Q}(\sqrt[r]{a}, \zeta_r)$ and for each prime q, let $L_{rq} = \mathbb{Q}(\sqrt[rq]{a}, \zeta_{rq})$. Then a famous theorem of Dedekind can be used to show that $R(p,q)$ holds if and only if p splits completely in L_{rq}. Thus, a has the required order for a given prime p if it splits in L_r, but not in L_{rq} for any prime

q. Since these fields are Galois extensions of $\mathbb{Q}$, the Chebotarev density theorem gives the proportion of primes that split completely in a given L_{rq}. Denoting the degree of the extensions L_k by n_k, the density of primes that split completely in L_k is $1/n_k$.

For any squarefree positive integer k let

$$L_{rk} = \prod_{q|k} L_{rq}$$

be the compositum of these fields, and n_{rk} denote the corresponding degree of the extension. Then the inclusion-exclusion principle and the Chebotarev density theorem lead one to conclude that the density of primes such that a has order $(p-1)/r$ modulo p should be

$$A(a,r) = \sum_{k=1}^{\infty} \frac{\mu(k)}{n_{rk}} \tag{1}$$

where $\mu(k)$ is the classical Möbius function.

This paper will show that under the generalised Riemann hypothesis, this is indeed the correct density. The next section analyses $A(a,r)$ in an attempt to express it in a more convenient form. Following this, the generalised Riemann hypothesis is used to compute an asymptotic formula for $\mathsf{N}_{\mathsf{a},\mathsf{r}}(x)$. We follow a method analogous to that originally implemented by Hooley to settle Artin's conjecture under the same hypothesis. Finally, in the fourth section we restrict our attention to a special case where it is possible to express $A(a,r)$ as a product and conclude that the primes in question have positive density. Subject to the generalised Riemann hypothesis, this verifies Golomb's claim about the density in these cases.

§2. Analysis of $A(a,r)$

We begin this section by attempting to relate the density for a general r to the case $r=1$, which corresponds to Artin's conjecture. Write $a = b^2c$ with c squarefree. Hooley showed that, if the generalised Riemann hypothesis holds, the density of primes given by Artin's conjecture is

$$A(a) = \delta \prod_q \left(1 - \frac{1}{n_q}\right) \tag{2}$$

where

$$\delta = \begin{cases} 1 - \mu(c)\prod_{q|c} \frac{1}{n_q - 1} & \text{if } c \equiv 1 \pmod 4 \\ 1 & \text{otherwise} \end{cases}$$

This gives the proportion of primes p such that p does not split in any L_q. Hence, by the Chebotarev density theorem, one would expect that the proportion of primes that don't split in each L_q with $(r,q)=1$, but do split in L_r is

$$\frac{A(a)}{n_r}\prod_{q|r}\left(1-\frac{1}{n_q}\right)^{-1}$$

Our initial remarks show that this is equivalent to the density of primes such that the index of a in $(\mathbb{Z}/p\mathbb{Z})^*$ is divisible by r, and divisible only by primes dividing r. The product must therefore be corrected in order to obtain the density of primes such that a has index precisely r. The inclusion-exclusion principle leads one to conclude that the correct density should be

$$A(a)\left(\sum_{k|r}\frac{\mu(k)}{n_{rk}}\right)\prod_{q|r}\left(1-\frac{1}{n_q}\right)^{-1} \tag{3}$$

In this Section 4 below, we will focus on a special case where $A(a,r)$ is in fact equal to the expression above.

For the remainder of this section k will denote a fixed squarefree positive integer. The following elementary lemma and induction show that $L_{rk}=\mathbb{Q}(\sqrt[rk]{a},\zeta_{rk})$.

Lemma 1. *Let K be a field and suppose that $a\in K$ has both m-th and n-th roots in K. Then a has an $mn/(m,n)$-th root in K.*

Proof. Suppose $c,d\in K$ satisfy $c^m=a$ and $d^n=a$. Let x,y be integers such that $xm'+yn'=1$, where $m'=m/(m,n)$ and $n'=n/(m,n)$. Then

$$a=a^{xm'}a^{yn'}=(d^xc^y)^{mn/(m,n)}\in K. \ \square$$

Put $Z=\mathbb{Q}(\zeta_{rk})$ and observe that in order to compute n_{rk} it suffices to compute $[L_{rk}\colon Z]$, for

$$n_{rk}=[L_{rk}\colon Z][Z\colon\mathbb{Q}]=[L_{rk}\colon Z]\phi(rk).$$

Let α be a root of the polynomial $x^{rk}-a$ and $F=\mathbb{Q}(\alpha)$, so that $L_{rk}=FZ$. Since the cyclotomic extension $Z/\mathbb{Q}$ is Galois, $[L_{rk}\colon Z]|[F\colon\mathbb{Q}]$. In light of this observation, we proceed to compute $[F\colon\mathbb{Q}]$. The following theorem will be useful.

Theorem 1. *Let K be a field, n an integer greater than 1 and $a\in K^*$. Assume that for all prime numbers $p|n$ we have $a\notin K^p$, and if $4|n$ then $a\notin -4K^4$. Then x^n-a is irreducible in $K[x]$.*

Proof. [10], p. 297. $\square$

This theorem and our assumptions about a imply that the polynomial $x^{rk}-a$ is irreducible. Hence, $[F\colon\mathbb{Q}]=rk$ and

$$rk=m[L_{rk}\colon Z]$$

for some integer m. In the sequel we will need to consider these extensions for a variety of values of k. Consequently, in these cases we will write $m(k) = m$ to denote the dependence on k.

Before moving on, we remark that the hypotheses imposed on a are only necessary for the application of Theorem 1 to the computation of $[F\colon \mathbb{Q}]$. For odd values of r it is possible to weaken these hypotheses. In the odd case, 4 does not divide rk for any squarefree k. Theorem 1 reveals that in this case the polynomial $x^{rk} - a$ is reducible if and only if a is a perfect p-th power for some prime $p|rk$. Thus, for odd values of r we need not assume a is positive, only that it is not a perfect power.

Let q be a prime divisor of m, and suppose that q does not divide r. The index $[Z(\sqrt[q]{a})\colon Z]$ is either 1 or q and, furthermore, it divides rk/m. Such primes q are relatively prime to rk/m, which shows that the index must be 1, and $\sqrt[q]{a} \in Z$. This cyclotomic field is abelian, and all subfields of it are abelian. Noting that the extension $\mathbb{Q}(\sqrt[q]{a})/\mathbb{Q}$ is Galois only when $q = 2$, one concludes that 2 is the sole possible prime divisor of m that does not divide r. Thus,

$$n_{rk} = \frac{\phi(rk)rk}{m}$$

for some $m|2r(r,k)$.

Galois theory shows that restricting automorphisms $\sigma \in \mathrm{Gal}(L_{rk}/F)$ to Z furnishes an isomorphism

$$\mathrm{Gal}(L_{rk}/F) \simeq \mathrm{Gal}(Z/(Z \cap F))$$

which yields the relation $m = [Z \cap F\colon \mathbb{Q}]$ ([10], p. 266). It will often be the case that $Z \cap F = \mathbb{Q}$ and $m = 1$. However, this is not always true; indeed, Artin's original miscalculation of the density of primes in the case $r = 1$ was due to an oversight of this fact! In the original Artin case, $m|2$, and this allows one to apply the theory of quadratic subfields of cyclotomic fields to find a neat criterion for determining the value of m. This remains true in our case, however, a different argument is necessary. The first result along these lines was worked out by Darbi in 1926 [2].

Theorem 2. *Let ζ_n denote a primitive n-th root of unity and let $x^n - a \in \mathbb{Q}[x]$ be irreducible with root α. Define an integer m as*

$$m = \max\{d \;:\; d|n \text{ and } \alpha^{n/d} \in \mathbb{Q}(\zeta_n)\}$$

Then the degree of the splitting field of $x^n - a$ is $n\phi(n)/m$.

Gay and Vélez [3] extended Darbi's result to fields of arbitrary characteristic. They also provided a more explicit formula for m applicable to the rational numbers. In particular, their work shows that in the present case

$$m = \begin{cases} 2 \text{ if } rk \text{ is even and } \sqrt{-a} \in \mathbb{Q}(\zeta_{2rk}) \\ 1 \text{ otherwise} \end{cases}$$

§3. Asymptotics for $\mathsf{N}_{\mathsf{a,r}}(x)$

Let π_r denote the set of primes that split completely in L_r, and similarly for π_{rq}. Equivalently, it is the set of primes p such that $R(p,1)$ (respectively $R(p,q)$) holds. Also let $\pi_{rk}(x)$ denote the number of primes no larger than x contained in $\bigcap_{q|k} \pi_{rq}$. In other words, $\pi_{rk}(x)$ gives the number of primes up to x that split in each L_{rq} for $q|k$. By convention take $\pi_r(x)$ to give the number of primes up to x contained in π_r. The inclusion-exclusion principle shows that

$$\mathsf{N}_{\mathsf{a,r}}(x) = \sum_{n=1}^{\infty} \mu(n)\pi_{rn}(x). \tag{4}$$

If $rq > x$ then $R(p,q)$ cannot possibly hold for any primes $p < x$. Hence, $\pi_{rq}(x)$ is zero for such primes q. This implies that the sum above is in fact finite.

In order to find an asymptotic formula for $\mathsf{N}_{\mathsf{a,r}}(x)$, we break the last sum up following Hooley's method for Artin's conjecture. Define another function $M(x;z,w)$ that counts the number of primes $p \leq x$ satisfying $R(p,q)$ for some prime q such that $z \leq rq \leq w$. Put $k = \prod_{rq \leq z} q$. The following upper bound is immediate

$$\mathsf{N}_{\mathsf{a,r}}(x) \leq \sum_{d|k} \mu(d)\pi_{rd}(x).$$

This is because the sum on the right counts all primes $p \leq x$ satisfying $R(p,1)$ and such that $R(p,q)$ does not hold for every prime q with $rq \leq z$. A lower bound is obtained just as easily using the function defined above

$$\mathsf{N}_{\mathsf{a,r}}(x) \geq \sum_{d|k} \mu(d)\pi_{rd}(x) - M(x;z,x).$$

These results lead us to the departure point of our asymptotic investigation

$$\mathsf{N}_{\mathsf{a,r}}(x) = \sum_{d|k} \mu(d)\pi_{rd}(x) + O(M(x;z,x)). \tag{5}$$

To continue the analysis we will require an effective version of the Chebotarev density theorem. Assuming the generalised Riemann hypothesis, one can prove that

$$\pi_{rd}(x) = \frac{1}{n_{rd}}\mathrm{Li}\ x + O(\sqrt{x}\log(rdx)). \tag{6}$$

where Li x is the logarithmic integral

$$\text{Li } x = \int_2^x \frac{dt}{\log t}$$

and the constant implied by the O notation is absolute [15]. Combining this result with (5) yields

$$\mathsf{N}_{\mathsf{a},\mathsf{r}}(x) = A(a,r)\text{Li } x - \left(\sum_{d \nmid k} \frac{\mu(d)}{n_{rd}}\right) \text{Li } x + \sum_{d|k} O\left(\sqrt{x}\log(rdx)\right) + O(M(x;z,x)).$$

Letting $z = (1/6)\log x$ gives

$$k = \prod_{rp \le z} p = e^{\theta(z/r)} \le e^{2z/r} \le x^{1/3}$$

which shows that the third term above is $O(x^{5/6}\log x)$. The results of the previous section can be applied to estimate the second term. The expression obtained for n_{rk} reveals that the term in question is

$$O\left(\sum_{d>z} \frac{\text{Li } x}{d\phi(d)}\right)$$

where the sum is over squarefree integers d. It is a well-known fact [7] that

$$\frac{d}{\phi(d)} < C \log\log d$$

for sufficiently large values of d. Hence,

$$O\left(\sum_{d>z} \frac{\text{Li } x}{d\phi(d)}\right) = O\left(\text{Li } x \sum_{d>z} \frac{\log\log d}{d^2}\right) = O\left(\frac{x\log\log x}{\log^2 x}\right).$$

The asymptotic expansion of Li x about infinity

$$\text{Li } x \sim \frac{x}{\log x} + \frac{x}{\log^2 x} + \frac{2!x}{\log^3 x} + \frac{3!x}{\log^4 x} + \cdots$$

allows one to rewrite the expression for $\mathsf{N}_{\mathsf{a},\mathsf{r}}(x)$:

$$\mathsf{N}_{\mathsf{a},\mathsf{r}}(x) = A(a,r)\frac{x}{\log x} + O\left(\frac{x\log\log x}{\log^2 x}\right) + O\left(M(x;z,x)\right). \tag{7}$$

To treat the $O(M(x;z,x))$ term, let $z_1 = \sqrt{x}/\log^2 x$ and $z_2 = \sqrt{x}\log x$. The inequality

$$M(x;z,x) \le M(x;z,z_1) + M(x;z_1,z_2) + M(x;z_2,x)$$

is used to break the estimation up into three tractable steps, each of which can be estimated following Hooley's original method.

The effective Chebotarev density theorem is used to treat $M(x; z, z_1)$. Observe that

$$M(x; z, z_1) \leq \sum_{z \leq rq \leq z_1} \pi_{rq}(x).$$

Substituting (6) into this inequality shows that

$$\begin{aligned} M(x; z, z_1) &\leq \text{Li } x \left(\sum_{z \leq rq \leq z_1} \frac{1}{n_{rq}} \right) + \sum_{z \leq rq \leq z_1} O\left(\sqrt{x} \log(rqx)\right) \\ &= O\left(\text{Li } x \left(\sum_{z \leq rq} \frac{1}{q(q-1)} \right) \right) + O\left(\sqrt{x} \log x \sum_{rq \leq z_1} 1 \right) \\ &= O\left(\frac{x}{\log^2 x} \right). \end{aligned}$$

The treatment of the second term begins similarly. As above, we have

$$M(x; z_1, z_2) \leq \sum_{z_1 \leq rq \leq z_2} \pi_{rq}(x).$$

The error term in the Chebotarev density theorem is too large for this case. A different approach must be used. Recall that the condition $R(p, q)$ contains two clauses. Maintaining only the condition that $p \equiv 1 \pmod{rq}$ provides the loose inequality

$$\pi_{rq}(x) \leq \sum_{\substack{p \leq x \\ rq | p-1}} 1.$$

This final term can be estimated via the Brun-Titchmarsh theorem ([12], p. 143). For large enough values of x,

$$\sum_{\substack{p \leq x \\ rq | p-1}} 1 \leq \frac{3x}{\phi(rq) \log(2x/rq)}$$

which leads one to the result that

$$M(x; z_1, z_2) = O\left(\frac{x}{\log x} \sum_{z_1 \leq rq \leq z_2} \frac{1}{\phi(q)} \right).$$

Following Hooley, an application of Merten's formula then gives

$$M(x; z_1, z_2) = O\left(\frac{x \log \log x}{\log^2 x} \right). \tag{8}$$

An elegant and very elementary argument is used for the final term. The key idea is that if $R(p,q)$ holds then p divides

$$a^{(p-1)/(rq)} - 1.$$

The inequalities $\sqrt{x}\log x \le rq$ and $p-1 < x$ yield $(p-1)/rq < \sqrt{x}/\log x$. Consequently, $M(x; z_2, x)$ is bounded by the number of distinct prime divisors of the product

$$\prod_{m<\sqrt{x}/\log x} (a^m - 1)\,.$$

Since $a^m - 1$ is divisible by at most $m\log a$ prime factors, this shows that

$$M(x; z_2, x) = O\left(\frac{x}{\log^2 x}\right).$$

These estimates prove the following theorem.

Theorem 3. *Let a be a positive integer that is not a p-th power for any prime p, and let r be a positive integer. If $\mathsf{N}_{\mathsf{a},\mathsf{r}}(x)$ denotes the number of primes $p \le x$ such that $p \equiv 1 \pmod r$ and a has order $(p-1)/r$ in $(\mathbb{Z}/p\mathbb{Z})^*$ then, assuming the generalised Riemann hypothesis,*

$$\mathsf{N}_{\mathsf{a},\mathsf{r}}(x) = A(a,r)\frac{x}{\log x} + O\left(\frac{x\log\log x}{\log^2 x}\right)$$

where

$$A(a,r) = \sum_{k>0} \frac{\mu(k)m(k)}{rk\phi(rk)}$$

and

$$m(k) = \begin{cases} 2 \textit{ if } rk \textit{ is even and } \sqrt{-a} \in \mathbb{Q}(\zeta_{2rk}) \\ 1 \textit{ otherwise} \end{cases}$$

§4. A Special Case

After making his conjecture, Golomb performed extensive computations for various values of r in the case $a = 2$. In this section we treat the case when r is odd, $a = b^2c$ is not a perfect p-th power for any prime p, and c is even and squarefree. This includes the case $a = 2$. The results established here match Golomb's computations.

Since r is odd, a remark from Section 2 shows that we need not assume a is positive. The same section showed that a full resolution to this problem depends upon determining when $\sqrt{-c} \in \mathbb{Q}(\zeta_{2rk})$ for squarefree k. First note that if k is odd then $\mathbb{Q}(\zeta_{2rk}) = \mathbb{Q}(\zeta_{rk})$. To see this one observes that $\mathbb{Q}(\zeta_{rk}) \subseteq \mathbb{Q}(\zeta_{2rk})$ and $[\mathbb{Q}(\zeta_{rk}) : \mathbb{Q}] = [\mathbb{Q}(\zeta_{2rk}) : \mathbb{Q}]$. The discriminant of the cyclotomic field $\mathbb{Q}(\zeta_{rk})$ divides $(rk)^{\phi(rk)}$, and is hence odd. These observations show that the rational prime 2 does not ramify in $\mathbb{Q}(\zeta_{2rk})$ when rk is odd. Hence, in these cases $\sqrt{-c} \notin \mathbb{Q}(\zeta_{2rk})$ and $m(k) = 1$.

The problem has been reduced to considering the case $k = 2t$. As above, we show that $\mathbb{Q}(\sqrt{-c})$ is not a quadratic subfield of $\mathbb{Q}(\zeta_{4rt})$. Quadratic subfields of a Galois extension correspond to subgroups of index 2 in the Galois group. The fields under consideration are not only Galois, but are in fact abelian. By considering group characters trivial on subgroups of index 2 in the Galois group, the duality theory of finite abelian groups furnishes a bijection between subgroups of index 2 and elements of order 2. Let s be the number of elements of order 2 in $(\mathbb{Z}/rt\mathbb{Z})^*$, so that $\mathbb{Q}(\zeta_{rt})$ has s quadratic subfields. Write them as $\mathbb{Q}(\sqrt{d_1}), \ldots, \mathbb{Q}(\sqrt{d_s})$ with the d_i's distinct integers. Since 2 does not ramify in $\mathbb{Q}(\zeta_{rt})$, upon consideration of the discriminant of the associated quadratic field one sees that $d_i \equiv 1 \pmod 4$ for each i. In particular, each d_i is odd.

The Chinese remainder theorem shows that $(\mathbb{Z}/4rt\mathbb{Z})^* \simeq (\mathbb{Z}/4\mathbb{Z})^* \times (\mathbb{Z}/rt\mathbb{Z})^*$ has $2s + 1$ elements of order 2. These correspond to the quadratic subfields

$$\mathbb{Q}(\sqrt{d_1}), \ldots, \mathbb{Q}(\sqrt{d_s}), \mathbb{Q}(\sqrt{-d_1}), \ldots, \mathbb{Q}(\sqrt{-d_s}), \mathbb{Q}(\sqrt{-1})$$

of $\mathbb{Q}(\zeta_{4rt})$. Since the d_i's are odd, one concludes that $\mathbb{Q}(\sqrt{-c})$ is not a quadratic subfield of $\mathbb{Q}(\zeta_{4rt})$ and $m(k) = 1$. Thus,

$$\begin{aligned} A(a,r) &= \sum_{k>0} \frac{\mu(k)}{rk\phi(rk)} = \sum_{d|r} \sum_{(k,r)=d} \frac{\mu(k)}{rk\phi(rk)} \\ &= \left(\sum_{d|r} \frac{\mu(d)}{rd\phi(rd)} \right) \left(\sum_{(k,r)=1} \frac{\mu(k)}{k\phi(k)} \right) \\ &= A(a) \left(\sum_{d|r} \frac{\mu(d)}{rd\phi(rd)} \right) \prod_{p|r} \left(1 - \frac{1}{p(p-1)} \right)^{-1} \end{aligned}$$

as predicted by (3) above (recall that $A(a)$ is Artin's constant). Rewrite the sum appearing in this expression as

$$\begin{aligned} \sum_{d|r} \frac{\mu(d)}{rd\phi(rd)} &= \frac{1}{r^2} \prod_{p|r} \left(\frac{p}{p-1} \right) \left(\sum_{d|r} \frac{\mu(d)}{d^2} \right) \\ &= \frac{1}{r^2} \prod_{p|r} \left(\frac{p}{p-1} \right) \prod_{p|r} \left(1 - \frac{1}{p^2} \right) \\ &= \frac{1}{r^2} \prod_{p|r} \left(1 + \frac{1}{p} \right). \end{aligned}$$

Hence, in this case

$$A(a,r) = \frac{A(a)}{r^2}\prod_{p\mid r}\left(\frac{p^2-1}{p^2-p-1}\right). \tag{9}$$

Equation (9) reveals that the density $A(a,r)$ is positive, which proves the following corollary of Theorem 3.

Corollary 1. *Let a be an integer that is not a p-th power for any prime p, and let r be an odd positive integer. Under the assumption of the generalised Riemann hypothesis, if $a = b^2c$ where c is even and squarefree, then there are infinitely many primes $p \equiv 1 \pmod r$ such that a has order $(p-1)/r$ in $(\mathbb{Z}/p\mathbb{Z})^*$.*

§5. Concluding Remarks

Golomb conjectured that, for any positive integer r, a given non-square integer $a > 1$ has index $(p-1)/r$ in $(\mathbb{Z}/p\mathbb{Z})^*$ for infinitely many primes $p \equiv 1 \pmod r$. Under the assumption of the generalised Riemann hypothesis, Theorem 3 is a good step towards a resolution of this conjecture. It can be improved in several important ways, many of which seem to depend upon a deeper understanding of the fields L_{rk}.

The work above assumes that a is positive and not a perfect p-th power. These simplifying assumptions imply that the polynomials $x^{rk} - a$ are irreducible, and the work of Gay and Vélez then provides a lower bound for $n_{rk} = [L_{rk} : \mathbb{Q}]$. If a suitable lower bound could be found for a more general class of integers a, the method of Hooley outlined in Section 3 could be applied to strengthen Theorem 3 to apply to these cases as well.

Theorem 3 does not allow one to conclude that Golomb's conjecture holds in any case. In particular, one is not able to conclude that the density (1) is positive. In the original Artin case, Hooley analysed the density and rewrote it as a product. This enabled him to conclude that it was positive. We achieved this for certain special cases of Golomb's conjecture in Section 4 above. A similar idea could be applied to the general case. It would require an explicit expression for n_{rk} akin to what Hooley achieved in his original work. One sees that treating Golomb's conjecture in the broadest generality is tantamount to computing the degree of the extension $\mathbb{Q}(\zeta_n, \sqrt[n]{a})/\mathbb{Q}$ for every positive integer n, and non-square integer $a \neq 0, 1, -1$. If this were known, it is expected that a simple application of the methods above would supply a proof of Golomb's conjecture under the assumption of the generalised Riemann hypothesis.

References

[1] E. Artin, *Collected Papers*, Addison-Wesley, 1965.

[2] G. Darbi, Sulla Riducibilita delle Equazioni Algebriche, *Annali di Math. pur e Appl.*, **4** (4) (1926) 185-208.

[3] D. Gay, W. Y. Vélez, On the Degree of the Splitting Field of an Irreducible Binomial, *Pacific J. of Math.*, **78** (1978), 117-120.

[4] S. W. Golomb, Letter to M. Ram Murty, June 22, 2004.

[5] S. W. Golomb, P.F. Lee, Which Irreducible Polynomials Divide Trinomials over GF(2)?, *SETA* (2004) 414-424.

[6] R. Gupta, M. Ram Murty, A Remark on Artin's Conjecture, *Inventiones Math.*, **78** (1984) 127-130.

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

[8] M. Harper and M. Ram Murty, Euclidean rings of algebraic integers, *Canadian Journal of Math.,* **56** (1) (2004), 71-76.

[9] C. Hooley, On Artin's Conjecture, *J. reine angew. Math.*, **226** (1967) 209-220.

[10] S. Lang, *Algebra*, Springer-Verlag, New York, 2002.

[11] S. Lang and H. Trotter, Primitive points on elliptic curves, *Bulletin of the Amer. Math. Soc.,* **83** (2) (1977), 289-292.

[12] M. Ram Murty, *Problems in Analytic Number Theory*, Springer-Verlag, New York, 2001.

[13] M. Ram Murty, Artin's Conjecture for Primitive Roots, *Math. Intelligencer*, **10** (4) (1988) 59-67.

[14] M. Ram Murty, On Artin's Conjecture, *Journal of Number Theory*, **16** (2) (1983) 147-168.

[15] M. Ram Murty, V. Kumar Murty, N. Saradha, Modular Forms and the Chebotarev Density Theorem, *American J. of Math.*, **110**(2) (1988) 253-281.

[16] J.-P. Serre, Résumé des course de 1977-1978, Annuaire du Collège de France, 67-70, (1978) in Collected Papers, Vol. 3, Springer-Verlag, 1985.

Cameron Franc and M. Ram Murty
Department of Mathematics
Queen's University, Kingston, Ontario, K7L3N6
Canada
E-mail: cfranc@math.mcgill.ca
E-mail: murty@mast.queensu.ca