Published in *Progress in Computer Science and Applied Logic* **20**, 33-41

Density Estimates Related to Gauß Periods

Joachim von zur Gathen and Francesco Pappalardi

Abstract. Given two integers q and k, for any prime r not dividing q with $r \equiv 1 \bmod k$, we denote by $\mathrm{ind}_r(q)$ the index of $q \bmod r$. In [2] the question was raised of calculating the density of the primes r for which $\mathrm{ind}_r(q)$ and $(r-1)/k$ are coprime; this is the condition that the Gauß period in $\mathbb{F}_{q^{(r-1)/k}}$ defined by these data be normal over $\mathbb{F}_q$. We assume the Generalized Riemann Hypothesis and calculate a formula for this density for all q and k. We prove unconditionally that our formula is an upper bound for the density and then express it as an Euler product. Finally we apply the results to characterize the existence of a special type of Gauß periods.

1. Introduction

Let q and k be integers with $|q| > 1$ and $k > 0$. For any prime r not dividing q, we define the index of $q \bmod r$ as $\mathrm{ind}_r(q) = [\mathbb{F}_r^* : \langle q \bmod r \rangle]$, so that $\mathrm{ind}_r(q) = (r-1)/\mathrm{ord}_r(q)$. If $r \equiv 1 \bmod k$, we also set

$$g_{q,k}(r) = \gcd\left(\mathrm{ind}_r(q), (r-1)/k\right).$$

Finally we let $M_{q,k}(x)$ be the number of primes $r \equiv 1 \bmod k$ up to x for which $g_{q,k}(r) = 1$.

The interest in this quantity comes from the construction of normal Gauß periods in $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$, where $q \in \mathbb{N}$ is a prime power. If $n = (r-1)/k$, $g_{q,k}(r) = 1$, $\beta \in \mathbb{F}_{q^{r-1}}$ is a primitive r–th root of unity, $K \subseteq \mathbb{F}_r^*$ is the unique subgroup of order k, and $\alpha = \sum_{i \in K} \beta^i$, then (n,k) is called in [2] a *Gauß pair* (over $\mathbb{F}_a$), and indeed the *Gauß period* α generates a normal basis for $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$. It was noted a few years ago that such a normal basis is useful for fast exponentiation in finite fields, which in turn has various cryptographic applications. Theory and applications of this, including implementations, are discussed in [2], [3], [4], [5], [6], [7]. A survey of these results is in [8]. In particular, two elements of $\mathbb{F}_{q^n}$ represented in such a basis can be multiplied at essentially the same cost as multiplying two polynomials of degree nk over $\mathbb{F}_q$.

Therefore a natural question is: given q and n as above, what is the smallest k such that (n,k) is a Gauß pair over $\mathbb{F}_q$?

In this paper we turn this question around and ask: given q and a (small) k, for how many n is (n, k) a Gauß pair over $\mathbb{F}_q$?

The paper [1] gives a generalization of Gauß periods, where basically the prime r is replaced by an arbitrary integer; our considerations only apply to the classical case as treated by Gauß, where $r = nk + 1$ is prime.

For $k = 1$, it is clear that $g_{q,k}(r) = 1$ if and only if $\operatorname{ind}_r(q) = 1$, and this happens exactly when q is a primitive root modulo r. Hence $M_{q,1}(x)$ is the number of primes r up to x for which q is a primitive root modulo r; the famous Artin Conjecture for primitive roots states that the set of these primes has a positive density unless q is a square or equals -1. In 1965, C. Hooley [11] proved that the Generalized Riemann Hypothesis implies the asymptotic formula

$$M_{q,1}(x) = \left(\delta_q + \mathrm{O}\left(\frac{\log\log x + \log q}{\log x}\right)\right)\frac{x}{\log x}$$

uniformly with respect to q, where δ_q depends only upon q. Unconditionally, the work of Gupta and Murty [9] and of Heath-Brown [10] provides evidence for the Artin Conjecture.

Our question can be considered as a natural generalization of Hooley's famous result. This generalization is meaningful also if q is a square.

For $r \in \mathbb{N}$, we let $\zeta_r \in \mathbb{C}$ be a primitive rth root of unity. We will prove the following results.

Theorem 1.1. *Let q and k be integers with $|q| > 1$ and $k > 0$, and for $m \in \mathbb{N}$ set $K_m = \mathbb{Q}(\zeta_{km}, q^{1/m})$ and $n_m = [K_m : \mathbb{Q}]$, and*

$$\delta_{q,k} = \sum_{1 \le m} \frac{\mu(m)}{n_m}.$$

Then there exists $c_{q,k} \in \mathbb{R}$ that depends only on q and k such that

$$M_{q,k}(x) \le \left(\delta_{q,k} + \frac{c_{q,k}}{\log\log x}\right)\frac{x}{\log x}.$$

If the Generalized Riemann Hypothesis holds for all these fields K_m, then

$$M_{q,k}(x) = \left(\delta_{q,k} + \mathrm{O}\left(\frac{\log\log x}{\log x}\right)\right)\frac{x}{\log x}.$$

Next we express the densities as Euler products. The parameter l in the products below ranges over the primes. We let

$$A = \prod_{l \text{ prime}} (1 - \frac{1}{l(l-1)}) \approx 0.373956$$

be Artin's constant, and μ the Möbius function.

Theorem 1.2. *With the notation of Theorem 1.1, we write* $q = b^h$ *and* $b = b_1^2 b_2$ *with integers* b, b_1, b_2, *and* h, *where* b *is not a perfect power and* b_2 *is squarefree, set*

$$b_3 = \begin{cases} 4b_2/\gcd(4b_2, k) & \text{if } b_2 \equiv 2, 3 \bmod 4, \\ b_2/\gcd(b_2, k) & \text{if } b_2 \equiv 1 \bmod 4, \end{cases}$$

write $b_3 = \alpha b_4$ *with* α *a power of two and* b_4 *odd, so that the values of* α *are given by the following table:*

	$2 \nmid k$	$2 \| k$	$4 \| k$	$8 \mid k$
$b_2 \equiv 1 \bmod 4$	1	1	1	1
$b_2 \equiv 3 \bmod 4$	4	2	1	1
$b_2 \equiv 2 \bmod 4$	8	4	2	1

.

Furthermore, we set

$$A_{h,k} = \frac{A}{k} \prod_{l \mid k} \left(1 + \frac{l}{l^2 - l - 1}\right) \prod_{\substack{l \mid h \\ l \nmid k}} \left(1 - \frac{l-1}{l^2 - l - 1}\right).$$

Then we have

$$\delta_{q,k} = A_{h,k} \cdot \left(1 - \frac{\mu(b_4 \cdot \gcd(h,2)^2) \cdot |\mu(\alpha)|}{2\gcd(2,k) - 1} \prod_{\substack{l \mid b_4 \\ l \nmid h}} \frac{1}{l^2 - l - 1} \prod_{\substack{l \mid b_4 \\ l \mid h}} \frac{1}{l-2}\right), \tag{1}$$

and $A_{h,k} = 0$ *if and only if* h *is even and* k *is odd.*

Finally we apply the above results to the problem of Gauß pairs.

Corollary 1.3. *Let* p *be a prime,* h *and* k *be positive integers,* $q = p^h$, *and assume that the GRH holds for all fields* K_m *of Theorem 1.1.*

(i) $\delta_{q,k} = 0$ *if and only if at least one of the following two conditions is satisfied:*
  (a) $2 \mid h$ *and* $2 \nmid k$,
  (b) $2 \nmid k$, $p \mid k$, *and* $p \equiv 1 \bmod 4$.

(ii) *If* $\delta_{q,k} = 0$, *then there is no Gauß pair* (n, k) *over* $\mathbb{F}_q$.

Proof. (i) We write (1) as $\delta_{q,k} = A_{h,k} \cdot B$, so that

$$\delta_{q,k} = 0 \iff A_{h,k} = 0 \text{ or } B = 0 \iff (2 \mid h \text{ and } 2 \nmid k) \text{ or } B = 0,$$

using Theorem 1.2. Furthermore,

$$B = 0 \iff \mu(b_4)|\mu(\alpha)| = (2\gcd(2,k) - 1) \prod_{\substack{l \mid b_4 \\ l \nmid h}} (l^2 - l - 1) \prod_{\substack{l \mid b_4 \\ l \mid h}} (l-2).$$

The left hand side has absolute value 1, and the right hand side is positive, since b_4 is odd. They are equal if and only if both are equal to 1. If that is the case, then $b_4 = 1$, since otherwise it would have at least two distinct prime factors, by $\mu(b_4) = 1$, and then one of the factors on the right hand side would be greater than 1. Since $|\mu(\alpha)| = 1$ if and only if $\alpha \leq 2$, we have

$$\begin{aligned} B = 0 \quad &\Longleftrightarrow \quad \alpha \leq 2, 2 \nmid k, b_4 = 1 \\ &\Longleftrightarrow \quad 2 \nmid k, \alpha = 1, b_3 = b_4 = 1, b_2 \equiv 1 \bmod 4 \\ &\Longleftrightarrow \quad 2 \nmid k, p \mid k, p \equiv 1 \bmod 4, \end{aligned}$$

since $b_2 = b = p$.

(ii) Since $\delta_{q,k} = 0$, either (a) or (b) holds. From (a) we find that $\mathrm{ind}_r(q)$ and $(r-1)/k$ are both even, so that $g_{q,k}(r)$ is even, for all odd primes r, and thus there is no Gauß pair (n, k) over $\mathbb{F}_q$. So now we assume that (b) holds, and let r be an odd prime with $r \equiv 1 \bmod k$. Then $(r-1)/k$ is even. Since p divides k, we also have $r \equiv 1 \bmod p$. We may assume that h is odd, since otherwise (a) holds. Then the quadratic reciprocity law gives the following for the Legendre symbol

$$\left(\frac{q}{r}\right) = \left(\frac{p^h}{r}\right) = \left(\frac{p}{r}\right) = \left(\frac{r}{p}\right) = \left(\frac{1}{p}\right) = 1.$$

Thus q is a square modulo r and $\mathrm{ind}_r(q)$ is even. Therefore again $g_{q,k}(r)$ is even, and there is no Gauß pair, as claimed. □

In particular, for q and k as in Corollary 1.3, the set of primes r for which $((r-1)/k, k)$ is a Gauß pair over $\mathbb{F}_q$ is either empty or has the positive density $\delta_{q,k}$.

Wassermann proves in [14] an existence result starting from a different set of parameters. His Theorem 3.3.4 states that for any given integers h, n and a prime p, there exists a Gauß pair (n, k) over $\mathbb{F}_{p^h}$ if and only if $\gcd(h, n) = 1$ and

$$\begin{aligned} &2p \nmid n \text{ if } p \equiv 1 \bmod 4, \\ &4p \nmid n \text{ if } p \equiv 2, 3 \bmod 4. \end{aligned}$$

2. Proof of the Theorems

The following lemma is the Chebotarev Density Theorem. The proof of the two versions that we state here is due to Lagarias and Odlyzko [12].

Lemma 2.1. *Suppose that L is a Galois extension of $\mathbb{Q}$ with absolute discriminant d_L and degree n_L over $\mathbb{Q}$, and define*

$$\pi(x, L\colon \mathbb{Q}) = \#\{p \leq x\colon p \text{ is unramified and splits completely in } L\}.$$

If the Generalized Riemann Hypothesis holds for the Dedekind zeta function of L, then

$$\pi(x, L\colon \mathbb{Q}) = \frac{1}{n_L}\,\mathrm{li}\,(x) + \mathrm{O}(x^{1/2}\log(x \cdot d_L^{1/n_L})).$$

In general (unconditionally) there exists absolute constants C_1 and B such that for

$$\sqrt{\log x} \geq C_1 \ n_L^{1/2} \max\{\log \mid d_L \mid, \mid d_L \mid^{1/n_L}\}, \tag{2}$$

one has

$$\pi(x, L\colon \mathbb{Q}) = \frac{1}{n_L}\operatorname{li}(x) + \mathrm{O}(x \exp(-Bn_L^{-1/2}\sqrt{\log x})).$$

□

Proof of Theorem 1.1. The argument is similar to the original one of Hooley, therefore we only mention the main steps.

We start by noticing that the condition for a prime $l \neq p$ to divide the index $\operatorname{ind}_p(q)$ is equivalent to p splitting completely in $\mathbb{Q}(\zeta_l, q^{1/l})$, while the condition that l divides $(p-1)/k$ is equivalent to p splitting completely in the cyclotomic field $\mathbb{Q}(\zeta_{lk})$. Since a prime splits completely in two extensions if and only if it splits completely in the compositum, by the inclusion–exclusion principle we gather that

$$M_{q,k}(x) = \sum_{1 \leq m} \mu(m)\pi(x, \mathbb{Q}(\zeta_{km}, q^{1/m})\colon \mathbb{Q}).$$

We now consider the set $S(y)$ of those squarefree "y-smooth" integers $m \geq 1$ all of whose prime divisors are less than a (sufficiently small) parameter y. We note that $S(y)$ has $2^{\pi(y)}$ elements, and if $m \in S(y)$, then $m \leq P(y)$, where $P(y)$ denotes the product of the primes up to y.

Furthermore, we let N and D denote the degree and the discriminant of K_m over $\mathbb{Q}$. Then $\sqrt{N} \leq \sqrt{k}m \leq \sqrt{k}P(y)$, $\log D \ll N \log N \ll yP(y)^2$, and $D^{1/N} \ll N \prod_{l \mid D} l \ll P(y)^3$, where the implied constants depend on a and k. By choosing y such that $P(y) = C_2(\log x)^{1/8}$ for some constant C_2, we can use the unconditional part of Lemma 2.1. The inclusion–exclusion principle then yields the (unconditional) upper bound

$$\begin{aligned}
M_{q,k}(x) &\leq \sum_{m \in S(y)} \mu(m)\pi(x, \mathbb{Q}(\zeta_{km}, q^{1/m})\colon \mathbb{Q}) \\
&= \sum_{m \in S(y)} \mu(m) \left\{ \frac{\operatorname{li}(x)}{n_m} + \mathrm{O}\left(x \exp(-C_3\sqrt{(\log x)/n_m})\right)\right\} \\
&= \left(\delta_{q,k} + \mathrm{O}\left(\sum_{m>y} \frac{1}{m\varphi(m)}\right)\right)\operatorname{li}(x) + \mathrm{O}\left(2^{\pi(y)} x \exp\left(-C_4 \frac{\sqrt{\log x}}{P(y)}\right)\right) \\
&= \left(\delta_{q,k} + \mathrm{O}\left(\frac{1}{y}\right)\right)\frac{x}{\log x} + \mathrm{O}\left(x \exp\left(-C_5(\log x)^{3/8}\right)\right) \\
&= \left(\delta_{q,k} + \mathrm{O}\left(\frac{1}{\log\log x}\right)\right)\frac{x}{\log x},
\end{aligned}$$

where we used the fact that $\varphi(m)m \ll n_m$. This proves the second part of Theorem 1.1. We note that the method of A. I. Vinogradov [13] could be used here to establish a sharper error term.

For the second claim we note that

$$\begin{aligned} M_{q,k}(x) &\leq \sum_{m \epsilon S(y)} \mu(m)\pi(x, \mathbb{Q}(\zeta_{km}, q^{1/m})\colon \mathbb{Q}) \\ &\leq M_{q,k}(x) + \#\left\{p \leq x \colon \exists l \geq y \quad l \mid g_{q,k}\right\}. \end{aligned}$$

Therefore

$$M_{q,k}(x) = \sum_{m \epsilon S(y)} \mu(m)\pi(x, \mathbb{Q}(\zeta_{km}, q^{1/m}) : \mathbb{Q}) + \mathrm{O}\left(\#\left\{p \leq x \colon \exists l \geq y \quad l \mid g_{q,k}\right\}\right).$$

The main term is estimated using the version of the Chebotarev Density Theorem in Lemma 2.1 dependent on the Generalized Riemann Hypothesis which leads to a choice of $y = \frac{1}{6}\log x$. The error term can be handled exactly as in Hooley's case, ignoring the condition that $l \mid (p-1)/k$. $\square$

For the proof of Theorem 1.2, we need the following two lemmas. We will have an integer h, and for an integer m we set

$$\hat{m} = m/\gcd(h, m).$$

Lemma 2.2. *Let $q, k, m \in \mathbb{Z}$ with $m, k > 0, |q| > 1$, and m squarefree. We write $q = b^h$ with b not a perfect power, $b = b_1^2 b_2$ with b_2 squarefree, and set*

$$\varepsilon = \begin{cases} 2 & \text{if } 2 \mid \hat{m}, b_2 \mid mk, \text{ and } b_2 \equiv 1 \bmod 4, \\ 2 & \text{if } 2 \mid \hat{m}, 4b_2 \mid mk, \text{ and } b_2 \not\equiv 1 \bmod 4, \\ 1 & \text{otherwise.} \end{cases}$$

Then $n_m = \varphi(km) \cdot \left[\mathbb{Q}(\zeta_{km}, q^{1/m}) : \mathbb{Q}\right] = \varphi(km)\hat{m}/\varepsilon$.

Proof. First we note that $\mathbb{Q}(\zeta_{km}, q^{1/m}) = \mathbb{Q}(\zeta_{km}, b^{1/\hat{m}})$. Since $[\mathbb{Q}(b^{1/\hat{m}}) : \mathbb{Q}] = \hat{m}$ and $[\mathbb{Q}(b^{1/\hat{m}})(\zeta_{km}) : \mathbb{Q}(b^{1/\hat{m}})]$ is a divisor of $\varphi(km)$, from the identity

$$[\mathbb{Q}(\zeta_{km}, b^{1/\hat{m}}) : \mathbb{Q}(\zeta_{km})] \cdot [\mathbb{Q}(\zeta_{km}) : \mathbb{Q}] = [\mathbb{Q}(b^{1/\hat{m}}, \zeta_{km}) : \mathbb{Q}(b^{1/\hat{m}})] \cdot [\mathbb{Q}(b^{1/\hat{m}}) : \mathbb{Q}]$$

we deduce that

$$n_m = \varphi(km)\left[\mathbb{Q}(\zeta_{km}, b^{1/\hat{m}}) : \mathbb{Q}(\zeta_{km})\right] = \varphi(km)\frac{\hat{m}}{d}$$

for some divisor d of $\hat{m}$. We claim that d is 1 or 2. Indeed, if l is a prime dividing d, then we have extensions

$$\mathbb{Q}(\zeta_{km}) \subseteq \mathbb{Q}(\zeta_{km}, b^{1/l}) \subseteq \mathbb{Q}(\zeta_{km}, b^{1/\hat{m}}).$$

Since $\hat{m}$ is squarefree, l does not divide $\hat{m}$, hence $\mathbb{Q}(\zeta_{km}, b^{1/l}) = \mathbb{Q}(\zeta_{km})$ and $b^{1/l} \in \mathbb{Q}(\zeta_{km})$. Therefore we have an inclusion of Abelian extensions $\mathbb{Q}(b^{1/l}) \subseteq \mathbb{Q}(\zeta_{km})$ of $\mathbb{Q}$. This can only happen when l is 1 or 2.

Furthermore $\mathbb{Q}(\sqrt{b}) = \mathbb{Q}(\sqrt{b_2})$, so that $d = 2$ if and only if $\hat{m}$ is even and $\sqrt{b_2} \in \mathbb{Q}(\zeta_{km})$.

The quadratic subfields of $\mathbb{Q}(\zeta_{km})$ are

$$\begin{array}{ll} \left\{\mathbb{Q}\left(\sqrt{\left(\frac{-1}{D}\right)|D|}\right) : D \mid km, D \text{ odd squarefree}\right\} & \text{if } 4 \nmid km, \\ \left\{\mathbb{Q}(\sqrt{D}) : D \mid km, D \text{ odd squarefree}\right\} & \text{if } 4 \,\|\, km, \\ \left\{\mathbb{Q}(\sqrt{D}) : D \mid km, D \text{ squarefree}\right\} & \text{if } 8 \mid km. \end{array}$$

In the first case, $d = 2$ if and only if $b_2|km$ and $b_2 \equiv 1 \bmod 4$, and in the second case, $d = 2$ if and only if b_2 is odd and divides km, and in the third case $d = 2$ if and only if $b_2|km$.

Finally, $d = \varepsilon$ and hence the claim. □

Lemma 2.3. *Let $A_{h,k}$ be as in the statement of Theorem 1.2 and $t \in \mathbb{N}$. Then*

$$A_{h,k} = \sum_{1 \le m} \frac{\mu(m)}{\varphi(km)\hat{m}} = \frac{1}{\varphi(k)} \prod_{l \text{ prime}} \left(1 - \frac{\gcd(l,h)\varphi(\gcd(l,k))}{l \gcd(l,k)(l-1)}\right),$$

$$\sum_{\substack{1 \le m \\ \gcd(m,t)=1}} \frac{\mu(m)}{\varphi(km)\hat{m}} = \frac{1}{\varphi(k)} \prod_{l \nmid t} \left(1 - \frac{\varphi(\gcd(l,k))}{(l-1)\hat{l}\gcd(l,k)}\right). \tag{3}$$

Proof. We have

$$\sum_{1 \le m} \frac{\mu(m)}{\varphi(km)\hat{m}} = \sum_{d|k} \sum_{\substack{1 \le m \\ \gcd(m,k)=d}} \frac{\mu(m)}{\varphi(km)\hat{m}}$$

$$= \left(\sum_{\substack{1 \le m \\ \gcd(m,k)=1}} \frac{\mu(m)}{\varphi(km)\hat{m}}\right) \cdot \left(\sum_{d|k} \frac{\mu(d)}{d\hat{d}}\right) = \frac{1}{\varphi(k)} \prod_{l \nmid k} \left(1 - \frac{1}{\hat{l}(l-1)}\right) \prod_{l|k} \left(1 - \frac{1}{\hat{l}l}\right),$$

since if $d \mid k$, then $\varphi(kmd) = d\varphi(km)$, and the claim is easily deduced. The second part is proven similarly. □

Let us now prove Theorem 1.2.

If h is even, then $\hat{m}$ is odd for any squarefree m, and this implies that $n_m = \varphi(km)\hat{m}$. Therefore by Lemma 2.3, we have that $\delta_{a,k} = A_{h,k}$. We now assume that h is odd (so that $\hat{m}$ is even if and only if m is), and consider b_3, b_4, and α as in the theorem. We note that $\gcd(b_4, k) = 1$. Furthermore, for any squarefree m, ε as defined in Lemma 2.2 equals 2 if and only if $\alpha \le 2$ and $2b_4|m$.

Therefore, if $\alpha \geq 4$, then $\delta_{q,k} = A_{h,k}$. If $\alpha \leq 2$, then

$$\delta_{q,k} = \sum_{2b_4 \nmid m} \frac{\mu(m)}{\varphi(km)\hat{m}} + 2\sum_{2b_4 \mid m} \frac{\mu(m)}{\varphi(km)\hat{m}} = A_{h,k} + \frac{\mu(2b_4)}{\widehat{2b_4}\varphi(b_4)} \sum_{\gcd(m,2b_4)=1} \frac{\mu(m)}{\varphi(2km)\hat{m}}.$$

By applying the multiplicative property (3) to the last sum above (with $t = 2b_4$ and $2k$ instead of k), we have

$$\delta_{q,k} = A_{h,k} - \frac{\mu(b_4)}{\widehat{2b_4}\varphi(b_4)\varphi(2k)} \prod_{l \nmid 2b_4} \left(1 - \frac{\varphi(\gcd(k,l))}{(l-1)\hat{l}\gcd(l,k)}\right).$$

In the inner product we write $\gcd(k,l)$ instead of $\gcd(2k,l)$, since l is odd. Now, we can factor out $A_{h,k}$ as follows. We multiply and divide the inner product by $\prod_{l \mid 2b_4} \left(1 - \frac{\varphi((k,l))}{\hat{l}\gcd(l,k)(l-1)}\right)$, and obtain:

$$\begin{aligned}
\delta_{q,k} = {} & A_{h,k} - \frac{\mu(b_4)}{\widehat{2b_4}\varphi(b_4)\varphi(2k)} \prod_{l} \left(1 - \frac{\varphi(\gcd(k,l))}{\hat{l}\gcd(l,k)(l-1)}\right) \\
& \cdot \prod_{l \mid 2b_4} \left(1 - \frac{\varphi(\gcd(k,l))}{\hat{l}\gcd(l,k)(l-1)}\right)^{-1} \\
= {} & A_{h,k} \left(1 - \frac{\mu(b_4)}{\widehat{2b_4}\varphi(b_4)} \frac{\varphi(k)}{\varphi(2k)} \prod_{l \mid 2b_4} \left(\frac{\hat{l}\gcd(l,k)(l-1)}{\hat{l}\gcd(l,k)(l-1) - \varphi(\gcd(k,l))}\right)\right).
\end{aligned}$$

It is easy to see that $\gcd(2,k)\varphi(k) = \varphi(2k)$ and $\hat{2} = 2$. If $l \mid b_4$, then $\gcd(l,k) = 1$, since $\gcd(b_4,k) = 1$. Therefore

$$\begin{aligned}
\delta_{q,k} = {} & A_{h,k} \left(1 - \frac{\mu(b_4)}{\widehat{2b_4}\varphi(b_4)} \frac{\varphi(k)}{\varphi(2k)} \prod_{l \mid 2} \left(\frac{\hat{l}\gcd(l,k)(l-1)}{\hat{l}\gcd(l,k)(l-1) - \varphi(\gcd(k,l))}\right)\right. \\
& \left. \cdot \prod_{l \mid b_4} \left(\frac{\hat{l}(l-1)}{\hat{l}(l-1) - 1}\right)\right) \\
= {} & A_{h,k} \left(1 - \frac{\mu(b_4)}{\widehat{2b_4}\varphi(b_4)} \frac{\varphi(k)}{\varphi(2k)} \frac{\hat{2}\gcd(2,k)}{\hat{2}\gcd(2,k) - 1}\right. \\
& \left. \cdot \prod_{l \mid b_4} \left(\hat{l}(l-1)\right) \prod_{l \mid b_4} \frac{1}{\hat{l}(l-1) - 1}\right) \\
= {} & A_{h,k} \left(1 - \frac{\mu(b_4)}{2\gcd(2,k) - 1} \prod_{l \mid b_4} \frac{1}{\hat{l}(l-1) - 1}\right).
\end{aligned}$$

Finally we can combine the three cases h even, h odd and $\alpha \geq 4$, and h odd and $\alpha \leq 2$, in a single formula as

$$\delta_{a,k} = A_{h,k} \left(1 - \frac{\mu(b_4 \cdot \gcd(h,2)^2)|\mu(\alpha)|}{2\gcd(2,k) - 1} \prod_{l|b_4} \frac{1}{\hat{l}(l-1) - 1} \right).$$

□

Acknowledgements The authors would like to thank Hans Roskam for having pointed out and corrected a mistake in Lemma 2.2 of the original version of the paper.

References

[1] S. Feisel, J. von zur Gathen, and M. A. Shokrollahi, *Normal bases via general Gauß periods*, Mathematics of Computation, **68**(225) (1999), 271–290.

[2] S. Gao, J. von zur Gathen, and D. Panario, *Gauss periods and fast exponentiation in finite fields*, In *Proceedings of LATIN '95,* Valparaíso, Chile, number 911 in Lecture Notes in Computer Science, 311–322, Springer-Verlag, 1995.

[3] S. Gao, J. von zur Gathen, and D. Panario, *Gauss periods: orders and cryptographical applications*, Mathematics of Computation, **67**(221) (1998), 343–352, Microfiche supplement.

[4] S. Gao, J. von zur Gathen, D. Panario, and V. Shoup, *Algorithms for exponentiation in finite fields*, Journal of Symbolic Computation **29**(6) (2000), 879–889.

[5] S. Gao and H. W. Lenstra, Jr. Optimal normal bases. *Designs, Codes, and Cryptography*, **2** (1992), 315–323.

[6] J. von zur Gathen and M. Nöcker, *Exponentiation in finite fields: Theory and practice*, In Teo Mora and Harold Mattson, editors, *Applied Algebra, Algebraic Algorithms and Error-Correcting Codes: AAECC-12,* Toulouse, France, number 1255 in Lecture Notes in Computer Science, 88–113, Springer-Verlag, 1997.

[7] J. von zur Gathen and M. Nöcker, *Computing special powers in finite fields: Extended abstract*, In Sam Dooley, editor, *Proceedings of the 1999 International Symposium on Symbolic and Algebraic Computation ISSAC '99,* Vancouver, Canada, 83–90, ACM Press, 1999.

[8] Joachim von zur Gathen and Igor Shparlinski, *Gauss periods in finite fields*, In *Proceedings Fq5* (2000), Birkhäuser Verlag, Basel. To appear.

[9] R. Gupta and M. R. Murty, *A remark on Artin's conjecture*, Invent. Math., **78** (1), (1984), 127–130.

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

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

[12] J. C. Lagarias and A. M. Odlyzko, *Effective versions of the Chebotarev Density Theorem in algebraic number fields,* in: *Algebraic Number Theory*, Ed. A. Fröhlich, Academic Press, New York 1977, 409–464.

[13] A. I. Vinogradov, *Artin L–series and his conjectures,* Proc. Steklov Inst. Math. **112** (1971), 124–142.

[14] Alfred Wassermann, *Zur Arithmetik in endlichen Körpern*, *Bayreuther Math. Schriften*, **44**, 147–251, 1993.

Fachbereich Mathematik-Informatik
Universität Paderborn
D–33095 Paderborn, Germany
E-mail: gathen@upb.de

Dipartimento di Matematica
Università Roma Tre
Largo S. L. Murialdo, 1
I–00146, Roma, Italy
E-mail: pappa@mat.uniroma3.it