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 \( r \equiv 1 \mod k \), we denote by \( \text{ind}_r(q) \) the index of \( q \mod r \). In \cite{2} the question was raised of calculating the density of the primes \( r \) for which \( \text{ind}_r(q) \) and \( (r-1)/k \) are coprime; this is the condition that the Gauß period in \( F_q^{(r-1)/k} \) defined by these data be normal over \( F_q \). 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 \( q \mod r \) as \( \text{ind}_r(q) = \{ F_r^*: (q \mod r) \} \), so that \( \text{ind}_r(q) = (r-1)/\text{ord}_r(q) \). If \( r \equiv 1 \mod k \), we also set

\[ g_{q,k}(r) = \gcd(\text{ind}_r(q), (r-1)/k). \]

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

The interest in this quantity comes from the construction of normal Gauß periods in \( F_q^* \) over \( F_q \), where \( q \in \mathbb{N} \) is a prime power. If \( n = (r-1)/k \), \( g_{q,k}(r) = 1 \), \( \beta \in F_{q^*} \) is the unique subgroup of order \( k \), and \( \alpha = \sum_{i \in K} \beta^i \), then \((n,k)\) is called in \cite{2} a Gauß pair (over \( F_q \)), and indeed the Gauß period \( \alpha \) generates a normal basis for \( F_{q^n} \) over \( F_q \). 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 \cite{2}, \cite{3}, \cite{4}, \cite{5}, \cite{6}, \cite{7}. A survey of these results is in \cite{8}. In particular, two elements of \( F_{q^n} \) represented in such a basis can be multiplied at essentially the same cost as multiplying two polynomials of degree \( nk \) over \( F_q \).

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 \( F_q \)?
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 \(\text{ind}_r(q) = 1\), 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

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

uniformly with respect to \(q\), where \(\delta_q\) 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 \(r\)th root of unity. We will prove the following results.

**Theorem 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

\[
\delta_{q,k} = \sum_{1 \leq m \leq n_m} \frac{\mu(m)}{n_m}
\]

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

\[
M_{q,k}(x) \leq \left( \delta_{q,k} + \frac{c_{q,k}}{\log \log x} \right) \frac{x}{\log x}.
\]

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

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

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

\[
A = \prod_{l \text{ prime}} \left( 1 - \frac{1}{l(l-1)} \right) \approx 0.373956
\]

be Artin’s constant, and \(\mu\) the Möbius function.
Theorem 1.2. With the notation of Theorem 1.1, we write \( q = b^h \) and \( b = b_1 b_2 \) with integers \( b, b_1, b_2, \) and \( h \), where \( b \) is not a perfect power and \( b_2 \) is squarefree, set
\[
b_3 = \begin{cases} 
4b_2 / \gcd(4b_2, k) & \text{if } b_2 \equiv 2, 3 \mod 4, \\
b_2 / \gcd(b_2, k) & \text{if } b_2 \equiv 1 \mod 4,
\end{cases}
\]
write \( b_3 = \alpha b_4 \) with \( \alpha \) a power of two and \( b_4 \) odd, so that the values of \( \alpha \) are given by the following table:

| \( b_2 \mod 4 \) | 2 \( \not| \) \( k \) | 2 \( | \) \( k \) | 4 \( | | \) \( k \) | 8 \( | \) \( k \) |
|------------------|----------------|----------------|----------------|----------------|
| 1                | 1              | 1              | 1              |                |
| 3                | 4              | 1              | 1              |                |
| 2                | 8              | 4              | 2              | 1              |

Furthermore, we set
\[
A_{h,k} = \frac{4}{k} \prod_{l \mid k} \left( 1 + \frac{l}{l^2 - l - 1} \right) \prod_{\ell \mid h} \left( 1 - \frac{1}{l^2 - l - 1} \right). 
\]

Then we have
\[
\delta_{q,k} = A_{h,k} \cdot \left( 1 - \frac{\mu(b_4 \cdot \gcd(h, 2))^2 \cdot |\mu(\alpha)|}{2 \gcd(2, k) - 1} \prod_{l \mid h} \frac{1}{l^2 - l - 1} \prod_{\ell \mid h} \frac{1}{l - 2} \right), \quad (1)
\]
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 \( 2 \not| \) \( k \),

(b) \( 2 \not| \) \( k \), \( p \mid k \), and \( p \equiv 1 \mod 4 \).

(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 \quad \text{or} \quad B = 0 \iff (2 \mid h \text{ and } 2 \not| \) \( k \) \text{ or } B = 0,
\]
using Theorem 1.2. Furthermore,
\[
B = 0 \iff \mu(b_4) \cdot |\mu(\alpha)| = (2 \gcd(2, k) - 1) \prod_{l \mid h} (l^2 - l - 1) \prod_{\ell \mid h} (l - 2).
\]
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
\[
B = 0 \iff \alpha \leq 2, 2 \not| k, b_4 = 1 \\
\iff 2 \not| k, \alpha = 1, b_3 = b_4 = 1, b_2 \equiv 1 \mod 4 \\
\iff 2 \not| k, p \mid k, p \equiv 1 \mod 4,
\]
since $b_2 = b = p$.
(ii) Since $\delta_{q,k} = 0$, either (a) or (b) holds. From (a) we find that $\text{ind}_r(q)$ 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 $r \equiv 1 \mod k$. Then $(r - 1)/k$ is even. Since $p$ divides $k$, we also have $r \equiv 1 \mod p$. We may assume that $h$ is odd, since otherwise (a) holds. Then the quadratic reciprocity law gives the following for the Legendre symbol
\[
\left(\frac{q}{r}\right) = \left(\frac{p^k}{r}\right) = \left(\frac{p}{r}\right) = \left(\frac{1}{p}\right) = 1.
\]
Thus $q$ is a square modulo $r$ and $\text{ind}_r(q)$ 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 $(r - 1)/k$ is a Gauß pair over $\mathbb{F}_q$ is either empty or has the positive density $\delta_{q,k}$.

Wasserman 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 $\mathbb{F}_p$ if and only if $\gcd(h,n) = 1$ and
\[
2p \not| n \text{ if } p \equiv 1 \mod 4, \\
4p \not| n \text{ if } p \equiv 2,3 \mod 4.
\]

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
\[
\pi(x,L: \mathbb{Q}) = \# \{ p \leq x : p \text{ is unramified and splits completely in } L \}.
\]
If the Generalized Riemann Hypothesis holds for the Dedekind zeta function of $L$, then
\[
\pi(x,L: \mathbb{Q}) = \frac{1}{n_L} \text{Li}(x) + O(x^{1/2} \log(x \cdot d_L^{1/n_L})�).\]
In general (unconditionally) there exists absolute constants $C_1$ and $B$ such that for
\[ \sqrt{\log x} \geq C_1 \, n_L^{1/2} \max \{\log |d_L|, |d_L|^{1/n_L}\}, \tag{2} \]
one has
\[ \pi(x, L; \mathbb{Q}) = \frac{1}{n_L} \text{li}(x) + O(x \exp(-B n_L^{-1/2} \sqrt{\log x})). \]

\[ \Box \]

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 $\text{ind}_p(q)$ 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 $\mathbb{Q}(\zeta_k)$. 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
\[ M_{q,k}(x) = \sum_{1 \leq m \leq x} \mu(m) \pi(x, \mathbb{Q}(\zeta_{km}, q^{1/m}); \mathbb{Q}). \]

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 $\sqrt{N} \leq \sqrt{d_m} \leq \sqrt{k} P(y)$, $\log D \ll N \log N \ll y P(y)^2$, and $D^{1/2} \ll N \prod_{l | D} l \ll P(y)^3$, where the implied constants depend on $a$ and $k$. By choosing $y$ such that $P(y) = C_2 (\log x)^{1/4}$ 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
\[ M_{q,k}(x) \leq \sum_{m \in S(y)} \mu(m) \pi(x, \mathbb{Q}(\zeta_{km}, q^{1/m}); \mathbb{Q}) \]
\[ = \sum_{m \in S(y)} \mu(m) \left\{ \frac{\text{li}(x)}{n_m} + O \left( x \exp\left(-C_3 \sqrt{(\log x)/n_m}\right) \right) \right\} \]
\[ = \left( \delta_{q,k} + O \left( \sum_{m > y} \frac{1}{m \varphi(m)} \right) \right) \text{li}(x) + O \left( 2^{\pi(y)} x \exp\left(-C_4 \sqrt{\log x}/P(y)\right) \right) \]
\[ = \left( \delta_{q,k} + O \left( \frac{1}{y} \right) \right) \frac{x}{\log x} + O \left( x \exp\left(-C_5 (\log x)^{3/4}\right) \right) \]
\[ = \left( \delta_{q,k} + O \left( \frac{1}{\log \log x} \right) \right) \frac{x}{\log x}, \]
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
\[
M_{q,k}(x) \leq \sum_{m \in S(y)} \mu(m) \pi(x, \mathbb{Q}(\zeta_{km}, q^{1/m}) : \mathbb{Q}) \leq M_{q,k}(x) + \# \{ p \leq x : \exists l \geq y \mid l \mid g_{q,k} \}.
\]

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

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 \( y = \frac{1}{2} \log x \). The error term can be handled exactly as in Hooley’s case, ignoring the condition that \( l \mid (p - 1)/k \).

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
\[
\varepsilon = \begin{cases} 
2 & \text{if } 2 \mid \hat{m}, b_2 \mid mk, \text{ and } b_2 \equiv 1 \mod 4, \\
2 & \text{if } 2 \mid \hat{m}, b_2 \mid mk, \text{ and } b_2 \equiv 1 \mod 4, \\
1 & \text{otherwise}.
\end{cases}
\]

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 \( \mathbb{Q}(\zeta_{km}, q^{1/m}) = \mathbb{Q}(\zeta_{km}, b^{1/h}) \). Since \( \left[ \mathbb{Q}(b^{1/h}) : \mathbb{Q} \right] = \hat{m} \) and \( \left[ \mathbb{Q}(b^{1/h})/\mathbb{Q}(\zeta_{km}) : \mathbb{Q}(b^{1/h}) \right] \) is a divisor of \( \varphi(km) \), from the identity 
\[
[\mathbb{Q}(\zeta_{km}, b^{1/h}) : \mathbb{Q}(\zeta_{km})] : [\mathbb{Q}(\zeta_{km}) : \mathbb{Q}] = [\mathbb{Q}(b^{1/h}, \zeta_{km}) : \mathbb{Q}(b^{1/h})] : [\mathbb{Q}(b^{1/h}) : \mathbb{Q}]
\]
we deduce that
\[
n_m = \varphi(km) \left[ \mathbb{Q}(\zeta_{km}, b^{1/h}) : \mathbb{Q}(\zeta_{km}) \right] = \varphi(km) \frac{\hat{m}}{d}
\]
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
\[
\mathbb{Q}(\zeta_{km}) \subseteq \mathbb{Q}(\zeta_{km}, b^{1/l}) \subseteq \mathbb{Q}(\zeta_{km}, b^{1/h}).
\]
Since \( \tilde{m} \) is squarefree, \( l \) does not divide \( \tilde{m} \), 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 \( \mathbb{Q}(\sqrt{b_1}) = \mathbb{Q}(\sqrt{b_2}) \), so that \( d = 2 \) if and only if \( \tilde{m} \) is even and \( \sqrt{b_2} \in \mathbb{Q}(\zeta_{km}) \).

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

\[
\begin{align*}
\mathbb{Q}(\sqrt{D}) & : D \mid km, D \text{ odd squarefree} & \text{if } 4 \nmid km, \\
\mathbb{Q}(\sqrt{D}) & : D \mid km, D \text{ odd squarefree} & \text{if } 4 \mid km, \\
\mathbb{Q}(\sqrt{D}) & : D \mid km, D \text{ squarefree} & \text{if } 8 \mid km.
\end{align*}
\]

In the first case, \( d = 2 \) if and only if \( b_2 \mid km \) and \( b_2 \equiv 1 \mod 4 \), 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 \( b_2 \mid km \).

Finally, \( d = 2 \) and hence the claim.

\[\square\]

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

\[
A_{h,k} = \sum_{1 \leq m \leq \varphi(k)m/m} \frac{\mu(m)}{\varphi(k)m/m} = \frac{1}{\varphi(k)} \prod_{l \text{ prime}} \left( 1 - \frac{\gcd(l, h) \varphi(\gcd(l, k))}{l \gcd(l, k)(l - 1)} \right), \]

\[
\sum_{\text{gcd}(m, r) = 1} \frac{\mu(m)}{\varphi(k)m/m} = \frac{1}{\varphi(k)} \prod_{l \nmid l} \left( 1 - \frac{\varphi(\gcd(l, k))}{(l - 1)l \gcd(l, k)} \right). \tag{3}
\]

**Proof.** We have

\[
\sum_{1 \leq m \leq \varphi(k)m/m} \frac{\mu(m)}{\varphi(k)m/m} = \sum_{d \mid k} \sum_{\text{gcd}(m, k) = d} \frac{\mu(m)}{\varphi(k)m/m}
\]

\[
= \left( \sum_{1 \leq m \leq \varphi(k)m/m} \frac{\mu(m)}{\varphi(k)m/m} \right) \cdot \left( \sum_{d \mid k} \frac{\mu(d)}{dd} \right) = \frac{1}{\varphi(k)} \prod_{l \nmid k} \left( 1 - \frac{1}{l(l - 1)} \right) \prod_{l \mid k} \left( 1 - \frac{1}{ll} \right),
\]

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

Let us now prove Theorem 1.2.

If \( h \) is even, then \( \tilde{m} \) is odd for any squarefree \( m \), and this implies that \( n_m = \varphi(k)m \). Therefore by Lemma 2.3, we have that \( \delta_{a,h} = A_{h,k} \). We now assume that \( h \) is odd (so that \( \tilde{m} \) is even if and only if \( m \) is), and consider \( b_3, b_4 \), and \( \alpha \) as in the theorem. We note that \( \gcd(b_4, k) = 1 \). Furthermore, for any squarefree \( m \), \( \varepsilon \) as defined in Lemma 2.2 equals 2 if and only if \( \alpha \leq 2 \) and \( 2b_4 \mid m \).
Therefore, if $\alpha \geq 4$, then $\delta_{q, k} = A_{h, k}$. If $\alpha \leq 2$, then

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

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

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

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 $\prod_{t \mid 2b_4} \left( 1 - \frac{\varphi(\gcd(k, l))}{\varphi(\gcd(l, k)) l} \right)$, and obtain:

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

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

$$
\delta_{q, k} = A_{h, k} \left( 1 - \frac{\mu(b_4)}{2b_4\varphi(b_4)\varphi(2k)} \prod_{t \mid 2} \left( \frac{\varphi(\gcd(k, l))}{\varphi(\gcd(l, k)) l} \right) \right)
\prod_{l \mid b_4} \left( \frac{\hat{l}(l - 1)}{l(l - 1) - 1} \right)
= A_{h, k} \left( 1 - \frac{\mu(b_4)}{2b_4\varphi(b_4)\varphi(2k)} \frac{2\gcd(2, k)}{2\gcd(2, k) - 1} \right)
\prod_{l \mid b_4} \left( \frac{\hat{l}(l - 1)}{l(l - 1) - 1} \right)
= A_{h, k} \left( 1 - \frac{\mu(b_4)}{2\gcd(2, k) - 1} \right) \prod_{l \mid b_4} \frac{1}{l(l - 1) - 1}.
$$
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
\[
\delta_{n,k} = A_{h,k} \left( 1 - \frac{\mu(b_4 \cdot \gcd(h, 2^2))|\mu(\alpha)|}{2 \gcd(2, k) - 1} \prod_{l | b_4} \frac{1}{l(l-1) - 1} \right).
\]

\[\square\]

**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**


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