MULTIPLICATIVE ORDERS OF GAUSS PERIODS AND THE ARITHMETIC OF REAL QUADRATIC FIELDS

FLORIAN BREUER

Abstract. We obtain divisibility conditions on the multiplicative orders of elements of the form $\zeta+\zeta^{-1}$ in a finite field by exploiting a link to the arithmetic of real quadratic fields.

1. Introduction

Let q be a prime number and n a positive integer. We denote by $\mathbb{F}_{q^n}$ the finite field of q^n elements. Suppose $p=2n+1$ is an odd prime number and let $\zeta \in \mathbb{F}_{q^{2n}}$ be a primitive p^{th} root of unity. We set

$$\alpha = \zeta + \zeta^{-1}.$$

Then $\alpha \in \mathbb{F}_{q^n}$ is known as a Gauss period of type $(n,2)$ over $\mathbb{F}_q$, and has many desirable properties. For example, when α is a primitive element, then it generates a normal basis for $\mathbb{F}_{q^n}$. As a result, one is interested in the multiplicative order $\operatorname{ord}(\alpha)$ of α in $\mathbb{F}_{q^n}^*$. See [ASV10, GS98, GV95, Pop12, Pop14] and the references therein, where amongst other things lower bounds on $\operatorname{ord}(\alpha)$ are obtained.

In this paper, we will look at divisibility conditions, which imply upper bounds. The trivial upper bound $\operatorname{ord}(\alpha) \leqslant q^n-1$ is often sharp when $q=2$ or 3, and in general the index $\operatorname{ind}(\alpha) := (q^n-1)/\operatorname{ord}(\alpha)$ tends to be small. The goal of this paper is to show how certain small prime factors of this index can be detected in the arithmetic of the real quadratic field $\mathbb{Q}(\sqrt{p})$.

More precisely, denote by ε_p and h_p the fundamental unit and class number of $K=\mathbb{Q}(\sqrt{p})$, respectively. Denote by $\mathcal{O}_K$ the ring of integers of K. When q is inert in $K/\mathbb{Q}$, we denote by $\operatorname{ind}(\varepsilon_p \bmod q)$ the multiplicative index of $(\varepsilon_p \bmod q\mathcal{O}_K)$ in $(\mathcal{O}_K/q\mathcal{O}_K)^* \cong \mathbb{F}_{q^2}^*$.

Our main result is the following.

2010 *Mathematics Subject Classification.* Primary: 11T30, Secondary: 11R11, 11R29.

Key words and phrases. Multiplicative orders, Gauss periods, class numbers, real quadratic units.

Theorem 1.1. *Let $p \equiv 5 \bmod 8$ be a prime number, suppose that $(\mathbb{Z}/p\mathbb{Z})^* = \langle -1, q\rangle$ and let $\zeta \in \mathbb{F}_{q^{p-1}}$ be a primitive p^{th} root of unity. Then*

$$\gcd\left(\operatorname{ind}(\zeta+\zeta^{-1}), q^2-1\right) = \operatorname{ind}(\varepsilon_p^{h_p} \bmod q).$$

Related elements of interest are $\beta = \zeta + 1 \in \mathbb{F}_{q^{2n}}$, whose multiplicative orders (when $q = 2$) determine periods of Ducci sequences, see [BLM07, Bre19, BS19]. When q is a primitive root modulo p, then $p \nmid (q^n - 1)$ so $p \nmid \operatorname{ord}(\zeta + \zeta^{-1})$ and we get

$$\operatorname{ord}(\zeta+1) = \operatorname{ord}(\zeta^2+1) = \operatorname{ord}\left(\zeta(\zeta+\zeta^{-1})\right) = p\operatorname{ord}(\zeta+\zeta^{-1}),$$

where we have used the fact that ζ and ζ^2 are conjugate.

Now, when $q = 2$ and $p \equiv 1 \bmod 4$, we find that $(\mathbb{Z}/p\mathbb{Z})^* = \langle -1, 2\rangle$ is equivalent to $(\mathbb{Z}/p\mathbb{Z})^* = \langle 2\rangle$. Theorem 1.1 implies

Corollary 1.2. *Suppose that $p \equiv 5 \bmod 8$ is prime and that 2 is a primitive root modulo p. Let $\zeta \in \mathbb{F}_{2^{p-1}}$ be a primitive pth root of unity. Then the following are equivalent:*

1. $\operatorname{ind}(\zeta+1)$ *is divisible by 3.*
2. $\operatorname{ind}(\zeta+\zeta^{-1})$ *is divisible by 3.*
3. *The eventual period P of any Ducci sequence in $\mathbb{Z}^p$ formed by iterating the map*

$$D : \mathbb{Z}^p \to \mathbb{Z}^p; \quad (x_1, x_2, \ldots, x_p) \mapsto (|x_1 - x_2|, |x_2 - x_3|, \ldots, |x_n - x_1|),$$

   satisfies $P | \frac{1}{3}p(2^{(p-1)/2} - 1)$.
4. *(i) $\varepsilon_p \equiv 1 \bmod 2\mathcal{O}_K$ or (ii) $3 | h_p$.*

This strengthens the main result of [Bre19], in which only the implication $4(i) \Rightarrow (3)$ was shown. The equivalence $(1) \Leftrightarrow (3)$ is shown in [BLM07].

2. Orders of fundamental units

We first record the following result, see for example [FT91, Cor. 2 to Thm. 39, p.182]

Lemma 2.1. *If $p \equiv 1 \bmod 4$ is prime, then $N_{K/\mathbb{Q}}(\varepsilon_p) = -1$ and h_p is odd.*

The following result is due to Ishikawa and Kitaoka.

Proposition 2.2. *Let $p \equiv 1 \bmod 4$ be a prime and suppose $q \nmid 2p$ is an inert prime in $K/\mathbb{Q}$. Then*

1. *$(q-1)/2$ divides $\operatorname{ind}(\varepsilon_p \bmod q)$*

(2) $\operatorname{ord}(\varepsilon_p \bmod q) \equiv \begin{cases} 4 \bmod 8 & \text{if } q \equiv 1 \bmod 4 \\ 0 \bmod 8 & \text{if } q \equiv 3 \bmod 4. \end{cases}$

In particular, $\operatorname{ord}(\varepsilon_p \bmod q) = \operatorname{ord}(-\varepsilon_p \bmod q)$.

Proof. Since $N_{K/\mathbb{Q}}(\varepsilon_p) = -1$ by Lemma 2.1, (1) follows from [IK98, Theorem 1.1], and (2) follows from [IK98, Corollary 1.4]. The final claim follows from the fact that $\operatorname{ord}(\varepsilon_p \bmod q)$ is divisible by 4. □

Proposition 2.2 and Theorem 1.1 imply that, if $q > 3$, then $\operatorname{ind}(\alpha)$ is divisible by $(q-1)/2$.

The possible values of the indices $\operatorname{ind}(\varepsilon_p \bmod q)$ for $q \leqslant 19$ inert in $\mathbb{Q}(\sqrt{p})/\mathbb{Q}$ and $p \equiv 1 \bmod 4$ are listed in Table 1. These values are computed as follows.

Since $p \equiv 1 \bmod 4$ we have

$$\mathcal{O}_K = \mathbb{Z}\left[\frac{1+\sqrt{p}}{2}\right] \cong \frac{\mathbb{Z}[X]}{\langle X^2 - X + \frac{1-p}{4}\rangle},$$

and under this isomorphism,

$$\varepsilon_p = \frac{x+y\sqrt{p}}{2} = \frac{1}{2}(x-y) + \left(\frac{1+\sqrt{p}}{2}\right) y \mapsto \frac{1}{2}(x-y) + Xy,$$

where x and y satisfy the Pellian equation

$$x^2 - py^2 = -4, \tag{2.1}$$

since $N_{K/\mathbb{Q}}(\varepsilon_p) = -1$ by Lemma 2.1.

Next, we consider the finite fields

$$\mathcal{O}_K/q\mathcal{O}_K \cong \frac{\mathbb{F}_q[X]}{\langle X^2 - X + \frac{1-p}{4}\rangle},$$

one for each residue class $p \bmod q$ such that q is inert in $K/\mathbb{Q}$. For odd q, we let p range through the quadratic non-residues mod q, by quadratic reciprocity, and when $q = 2$ we set $p = 5$.

For each $a+bX$ in such a field, we check whether $a+bX = \frac{1}{2}(x-y)+Xy$ holds with x, y satisfying (2.1). If so, we compute its multiplicative index and we have found a candidate value for $\operatorname{ind}(\varepsilon_p \bmod q)$. The proportion of candidate residue classes for each multiplicative index gives a naïve prediction for the density of primes p for which $\operatorname{ind}(\varepsilon_p \bmod q)$ equals that index. These predictions, together with the observed density for primes $p \equiv 1 \bmod 4$, $p < 10^8$ are shown in Table 1. (Restricting to primes $p \equiv 5 \bmod 8$ produces similar results).

Lastly, the consequences for $\operatorname{ind}(\alpha)$ from Theorem 1.1 are also listed, using the fact that h_p is odd.

q	$i(\varepsilon_p \bmod q)$	Freq. pred.	Freq. obs.	Consequences of Theorem 1.1
2	1	$\frac{2}{3}$	0.67497	$3 \mid \mathrm{ind}(\alpha)$ iff $3 \mid h_p$
	3	$\frac{1}{3}$	0.32503	$3 \mid \mathrm{ind}(\alpha)$
3	1	1	1.0	$2 \nmid \mathrm{ind}(\alpha)$
5	2	$\frac{2}{3}$	0.67359	$2 \parallel \mathrm{ind}(\alpha)$, and $3 \mid \mathrm{ind}(\alpha)$ iff $3 \mid h_p$
	6	$\frac{1}{3}$	0.32641	$2 \parallel \mathrm{ind}(\alpha)$ and $3 \mid \mathrm{ind}(\alpha)$
7	3	1	1.0	$2 \nmid \mathrm{ind}(\alpha)$, and $3 \mid \mathrm{ind}(\alpha)$
11	5	$\frac{2}{3}$	0.67325	$2 \nmid \mathrm{ind}(\alpha)$, $5 \mid \mathrm{ind}(\alpha)$, and $3 \mid \mathrm{ind}(\alpha)$ iff $3 \mid h_p$
	15	$\frac{1}{3}$	0.32675	$2 \nmid \mathrm{ind}(\alpha)$ and $15 \mid \mathrm{ind}(\alpha)$
13	6	$\frac{6}{7}$	0.85795	$2 \parallel \mathrm{ind}(\alpha)$, $3 \mid \mathrm{ind}(\alpha)$, and $7 \mid \mathrm{ind}(\alpha)$ iff $7 \mid h_p$
	42	$\frac{1}{7}$	0.14205	$2 \parallel \mathrm{ind}(\alpha)$ and $21 \mid \mathrm{ind}(\alpha)$
17	8	$\frac{2}{3}$	0.67236	$2^3 \parallel \mathrm{ind}(\alpha)$, $3 \parallel \mathrm{ind}(\alpha)$ iff $3 \parallel h_p$, and $9 \mid \mathrm{ind}(\alpha)$ iff $9 \mid h_p$
	24	$\frac{2}{9}$	0.21849	$2^3 \parallel \mathrm{ind}(\alpha)$, $3 \parallel \mathrm{ind}(\alpha)$ iff $3 \nmid h_p$, and $9 \mid \mathrm{ind}(\alpha)$ iff $3 \mid h_p$
	72	$\frac{1}{9}$	0.10914	$2^3 \parallel \mathrm{ind}(\alpha)$ and $9 \mid \mathrm{ind}(\alpha)$
19	9	$\frac{4}{5}$	0.80082	$2 \nmid \mathrm{ind}(\alpha)$, $9 \mid \mathrm{ind}(\alpha)$ and $5 \mid \mathrm{ind}(\alpha)$ iff $5 \mid h_p$
	45	$\frac{1}{5}$	0.19918	$2 \nmid \mathrm{ind}(\alpha)$ and $45 \mid \mathrm{ind}(\alpha)$

TABLE 1. Possible values of $\mathrm{ind}(\varepsilon_p \bmod q)$ for small q and various p. The third and fourth columns list the predicted and observed frequency, respectively, of each given value of $\mathrm{ind}(\varepsilon_p \bmod q)$ for primes $p \equiv 1 \bmod 4$, $p < 10^8$.

We illustrate this with the example $q = 5$. We consider the finite fields $F_2 = \mathbb{F}_5[X]/\langle X^2 - X - 4\rangle$ and $F_3 = \mathbb{F}_5[X]/\langle X^2 - X - 3\rangle$, corresponding to the residue classes $p \equiv 2$ and $3 \bmod 5$, respectively. In F_2 there are 6 elements $aX + b$ satisfying $(2a + b)^2 - 2b^2 \equiv -4 \bmod q$, which thus might represent $\varepsilon_p \bmod 5\mathcal{O}_K$. Four of them, $2X, 3X, 2X+3$

and $3X+2$, have multiplicative index 2 while the elements 2 and 3 in F_2 have multiplicative index 6. The situation is similar in F_3. Thus we predict that $\operatorname{ind}(\varepsilon_p \bmod 5)$ equals 2 with probability 2/3 and equals 6 with probability 1/3.

Theorem 1.1 says that $\gcd\big(\operatorname{ind}(\alpha), 24\big) = \operatorname{ind}(\varepsilon_p^{h_p} \bmod 5)$. It follows that $2 \| \operatorname{ind}(\alpha)$, since h_p is odd. Furthermore, $3 | \operatorname{ind}(\alpha)$ if and only if $3 | h_p$ or $\operatorname{ind}(\varepsilon_p \bmod 5) = 6$.

It would be interesting to prove that the predicted densities in Table 1 are indeed correct, but nothing seems to be known rigorously. Even the question of whether there are infinitely many primes $p \equiv 5 \bmod 8$ for which $\operatorname{ind}(\varepsilon_p \bmod 2) = 3$ is still open, although there are some known results if we relax the condition p prime to p squarefree, see [Ste96].

On the other hand, in the related situation in which p is fixed and q varies, more is known. In particular, densities of q for which $\operatorname{ind}(\varepsilon_p \bmod q)$ equals a given value are obtained in [CKY00, Kat03] under the assumption of the generalized Riemann Hypothesis.

3. Proof of the main result

From now on, we fix a prime number $p \equiv 5 \bmod 8$.

Let $\zeta_p = \exp(2\pi i/p) \in \mathbb{C}$ be a primitive p^{th} root of unity, $L = \mathbb{Q}(\zeta_p)$ the corresponding cyclotomic number field and $L^+ = \mathbb{Q}(\zeta_p + \zeta_p^{-1})$ its maximal totally real subfield. Now $K = \mathbb{Q}(\sqrt{p})$ is the unique quadratic subfield of L^+.

We denote by $\mathcal{O}_L$ and $\mathcal{O}_{L^+}$ the rings of integers of L and L^+, respectively. Our elements $\alpha \in \mathbb{F}_{q^n}$ are the reductions of the unit $\zeta_p + \zeta_p^{-1} \in \mathcal{O}_{L^+}^*$ modulo primes lying above q.

The following result determines the norms $N_{L/K}(\zeta_p+1)$ and $N_{L^+/K}(\zeta_p+\zeta_p^{-1})$ in K. It is one of many consequences of Dirichlet's Class Number Formula for K; we prove it here for lack of a suitable reference.

Proposition 3.1. *Suppose $p \equiv 5 \bmod 8$. Then*

$$(1)\quad N_{L/K}(\zeta_p + 1) = \prod_{k=1}^{(p-1)/2} \big(\zeta_p^{k^2} + 1\big) = \varepsilon_p^{-2h_p}.$$

$$(2)\quad N_{L^+/K}(\zeta_p + \zeta_p^{-1}) = \prod_{0<r\leqslant \frac{p-1}{2}, \left(\frac{r}{p}\right)=1} \big(\zeta_p^r + \zeta_p^{-r}\big) = (-1)^m \varepsilon_p^{h_p},$$

where

$$\begin{aligned} m &= \#\{r \mid \frac{p+3}{4} \leqslant r \leqslant \frac{p-1}{2},\ \left(\frac{r}{p}\right) = 1\} \\ &= \frac{1}{4}\left[\frac{p-1}{2} - h(-p)\right] \end{aligned}$$

and $h(-p)$ is the class number of the imaginary quadratic field $\mathbb{Q}(\sqrt{-p})$.

Proof. First note that

$$\begin{aligned} N_{L/K}(\zeta_p + 1) &= \prod_{\sigma \in \mathrm{Gal}(L/K)} \left(\sigma(\zeta) + 1\right) \\ &= \prod_{0<r\leqslant p-1, \left(\frac{r}{p}\right)=1} \left(\zeta^r + 1\right) = \prod_{k=1}^{(p-1)/2} \left(\zeta_p^{k^2} + 1\right) \end{aligned}$$

and

$$N_{L^+/K}(\zeta_p + \zeta_p^{-1}) = \prod_{\sigma \in \mathrm{Gal}(L^+/K)} \left(\sigma(\zeta_p) + \sigma(\zeta_p^{-1})\right) = \prod_{0<r\leqslant \frac{p-1}{2}, \left(\frac{r}{p}\right)=1} (\zeta_p^r + \zeta_p^{-r}).$$

A particularly elegant form of Dirichlet's analytic class number formula for K is [FT91, Thm. 71, p.309]

$$\prod_{k=1}^{(p-1)/2} \left(\zeta_p^k - \zeta_p^{-k}\right)^{-\left(\frac{k}{p}\right)} = \varepsilon_p^{h_p}.$$

Set $R = \{r \in \mathbb{Z} \mid 0 < r \leqslant \frac{p-1}{2},\ \left(\frac{r}{p}\right) = 1\}$ and $N = \{n \in \mathbb{Z} \mid 0 < n \leqslant \frac{p-1}{2},\ \left(\frac{n}{p}\right) = -1\}$. Since $\left(\frac{2}{p}\right) = -1$, we have

$$\begin{aligned} \varepsilon_p^{h_p} &= \frac{\prod_{n\in N}\left(\zeta_p^n - \zeta_p^{-n}\right)}{\prod_{r\in R}\left(\zeta_p^r - \zeta_p^{-r}\right)} = \frac{\prod_{r\in R^*}\left(\zeta_p^{2r} - \zeta_p^{-2r}\right)}{\prod_{r\in R}\left(\zeta_p^r - \zeta_p^{-r}\right)} \\ &= \frac{\prod_{r\in R^*}\left(\zeta_p^r - \zeta_p^{-r}\right)}{\prod_{r\in R}\left(\zeta_p^r - \zeta_p^{-r}\right)} \cdot \prod_{r\in R^*}\left(\zeta_p^r + \zeta_p^{-r}\right) = \pm \prod_{r\in R}\left(\zeta_p^r + \zeta_p^{-r}\right), \end{aligned}$$

where R^* is another set of representatives of quadratic residues modulo p up to ± 1. This proves (2) up to a sign, which we determine next.

We have $\varepsilon_p^{h_p} > 0$, whereas the number of negative factors in $\prod(\zeta_p^r + \zeta_p^{-r}) = \prod 2\cos(2\pi ir/p)$ equals

$$\begin{aligned} m &= \#\{r \mid \frac{p}{4} < r < \frac{p}{2},\ \left(\frac{r}{p}\right) = 1\} \\ &= \frac{p-1}{4} - \#\{r \mid 0 < r < \frac{p}{4},\ \left(\frac{r}{p}\right) = 1\} \\ &= \frac{p-1}{4} - \frac{1}{2}\sum_{r=1}^{(p-1)/4}\left[1 + \left(\frac{r}{p}\right)\right] \\ &= \frac{p-1}{4} - \frac{1}{2}\left[\frac{p-1}{4} + \sum_{r=1}^{(p-1)/4}\left(\frac{r}{p}\right)\right] \\ &= \frac{1}{4}\left[\frac{p-1}{2} - h(-p)\right], \end{aligned}$$

by Dirichlet's class number formula for $h(-p)$, [Dir99, §106].

To show (1), we note that ζ_p and ζ_p^2 are non-conjugates over K, so

$$\begin{aligned} N_{L/K}(\zeta_p + 1) &= \overline{N_{L/K}(\zeta_p^2 + 1)} = \overline{N_{L/K}(\zeta_p) N_{L/K}(\zeta_p + \zeta_p^{-1})} \\ &= 1 \cdot \overline{\left(N_{L^+/K}(\zeta_p + \zeta_p^{-1})\right)^2} = \overline{\varepsilon_p^{2h_p}} = \varepsilon_p^{-2h_p}. \end{aligned}$$

□

Remark 3.2. *The above considerations are quite similar to those in* [Cho68].

Now suppose that $(\mathbb{Z}/p\mathbb{Z})^* = \langle -1, q\rangle$. Then q is inert in $L^+/\mathbb{Q}$ and so the following diagram commutes, where the horizontal arrows are reduction modulo q and the vertical arrows are norms.

$$\begin{array}{ccccc} \zeta_p + \zeta_p^{-1} & \in & \mathcal{O}_{L^+}^* & \longrightarrow & \left(\mathcal{O}_{L^+}/q\mathcal{O}_{L^+}\right)^* \\ \big\downarrow & & \big\downarrow{\scriptstyle N_{L^+/K}} & & \big\downarrow{\scriptstyle N} \\ \pm\varepsilon_p^{h_p} & \in & \mathcal{O}_K^* & \longrightarrow & \left(\mathcal{O}_K/q\mathcal{O}_K\right)^* \end{array} \tag{3.1}$$

Here, $N(\alpha) = \pm\varepsilon_p^{h_p} \bmod q\mathcal{O}_K$, where the sign is irrelevant for the multiplicative index by Proposition 2.2.

Theorem 1.1 now follows from the following lemma, where for an element g of a finite group G, we denote by $\operatorname{ord}_G(g)$ its order and by $\operatorname{ind}_G(g) = \#G/\operatorname{ord}_G(g)$ its index.

Lemma 3.3. *Let $f : G \twoheadrightarrow H$ be an epimorphism of finite cyclic groups and $g \in G$. Then* $\mathrm{ind}_H(f(g)) = \gcd(\mathrm{ind}_G(g), |H|)$

Proof. For every divisor d of $|H|$, denote by $H_d < H$ and $G_d < G$ the unique subgroup of index d. Let ℓ be a prime number dividing $|H|$ and let $n = v_\ell(|H|)$ be the ℓ-adic valuation of $|H|$. Then for every $0 \leqslant i \leqslant n$, the map f restricts to an epimorphism $f : G_{\ell^i} \twoheadrightarrow H_{\ell^i}$. Now

$$\begin{aligned} v_\ell(\mathrm{ind}_G(g)) = m \quad &\iff \quad g \in G_{\ell^m} \smallsetminus G_{\ell^{m+1}} \\ &\iff \quad f(g) \in H_{\ell^m} \smallsetminus H_{\ell^{m+1}} \\ &\iff \quad v_\ell(\mathrm{ind}_H(f(g))) = m. \end{aligned}$$

The result follows. □

4. Some heuristics

How often does a given prime divide $\mathrm{ord}(\alpha)$?

Suppose $d | q^n - 1$. Then a randomly chosen element $\beta \in \mathbb{F}_{q^n}^*$ satisfies $d | \mathrm{ind}(\beta)$ with probability $1/d$, since $\mathbb{F}_{q^n}^*$ has a unique subgroup of index d.

In the case $q = 2$ and $p \equiv 5 \bmod 8$, a naïve heuristic (e.g. [Bre19, §4]) suggests that $\varepsilon_p \equiv 1 \bmod 2$ occurs with probability $1/3$, whereas the Cohen-Lenstra heuristics [CL84, §9.II] predict that $3 | h_p$ with probability $1 - \prod_{k \geqslant 2}(1 - 3^{-k}) \approx 0.159811$. Assuming that these conditions are independent, we thus expect the index $\mathrm{ind}(\zeta + \zeta^{-1})$ to be divisible by 3 for about 43.9874% of primes $p \equiv 5 \bmod 8$ for which 2 is a primitive root.

This suggests that the Gauss period $\alpha = \zeta + \zeta^{-1} \in \mathbb{F}_{2^n}^*$ is at least 10% less likely to be a primitive root than a randomly chosen element, due to the potential 3-divisibility of the class number h_p.

Lastly, we consider the case where $p = 2r + 1$ and r is also prime, in which case r is called a Sophie Germain prime. Since $[\mathbb{Q}(\zeta_p + \zeta_p^{-1}) : \mathbb{Q}] = r$ is prime, there are no intermediate fields K for which a phenomenon like Theorem 1.1 might occur. In this case, a conjecture of Gao and Vanstone [GV95] states that the Gauss period $\alpha \in \mathbb{F}_{2^r}^*$ is always a primitive root. The conjecture is verified in [GV95] for $r < 593$.

We give some heuristic arguments supporting this conjecture.

Assuming the Gauss period α behaves like a random element of $\mathbb{F}_{2^r}^*$, any prime divisor ℓ of $2^r - 1$ will divide $\mathrm{ind}(\alpha)$ with probability $1/\ell$. What is the probability that ℓ divides $2^r - 1$? Naïvely, we expect $1/\ell$ also. Less Naïvely, we may argue as follows (see e.g. [Wag83]).

Every prime divisor $\ell | 2^r - 1$ (where r is prime) must be of the form $\ell = 2kr + 1$, where $k \equiv 0$ or $-r \bmod 4$. The proportion of primes of

this form is $\frac{1}{2}\frac{1}{\varphi(2r)} \approx \frac{1}{2r}$. By a heuristic argument from [SK67], each such prime has probability $1/k \approx 2r/\ell$ of dividing $2^r - 1$. Combining these, we again find that a prime $\ell > 2r$ divides $2^r - 1$ with probability $1/\ell$.

The expected number of counter-examples to the conjecture of Gao and Vanstone is thus less than

$$\sum_{\substack{r \geqslant 593 \\ r \text{ Sophie Germain prime}}} \sum_{\substack{\ell > 2r \\ \ell \text{ prime}}} \frac{1}{\ell^2} \approx \sum_{r=593}^{\infty} \frac{2C}{\log^2 r} \sum_{l=2r+1}^{\infty} \frac{1}{l^2 \log l}$$

$$\approx \int_{593}^{\infty} \frac{2C}{\log^2 r} \left(\int_{2r+1}^{\infty} \frac{1}{l^2 \log l}\, dl \right) dr \approx 0.007.$$

Here we have used the heuristic that r is a Sophie Germain prime with probability $2C/\log^2 r$, where $C \approx 0.66$ is the Hardy-Littlewood twin prime constant.

Acknowledgements. The author would like to thank Pieter Moree and Igor Shparlinski for helpful comments, and an anonymous referee for pointing out an error in Proposition 3.1. Part of this research was carried out at the Universität Heidelberg with generous funding by the Alexander-von-Humboldt Foundation.

References

[ASV10] O. Ahmadi, I. E. Shparlinski and J. F. Voloch, Multiplicative order of Gauss periods, *Internat. J. Number Theory* **6** (2010) no. 4, 877–882. 1

[BLM07] F. Breuer, E. Lötter and A.B. van der Merwe, Ducci sequences and cyclotomic polynomials, *Finite Fields Appl.* **13** (2007), 293–304. 2

[Bre19] F. Breuer, Periods of Ducci sequences and odd solutions to a Pellian equation, *Bull. Aust. Math. Soc.*, **100** (2019), 201–205 doi:10.1017/S0004972719000212 2, 8

[BS19] F. Breuer and I. E. Shparlinski, Lower bounds for periods of Ducci sequences, *Bull. Aust. Math. Soc.*, To appear. 2

[CKY00] Y.-M. Chen, Y. Kitaoka and J. Yu, Distribution of units of real quadratic number fields, *Nagoya Math. J.* **158** (2000), 167–184. 5

[Cho68] P. Chowla, On the class-number of real quadratic fields, *J. Reine Angew. Math.* **230** (1968), 51–60. 7

[CL84] H. Cohen and H. W. Lenstra, Heuristics on class groups of number fields, in: *Number Theory Noordwijkerhout 1983*, 33–62, Springer-Verlag, 1984. 8

[Dir99] P.G.L. Dirichlet, Lectures on Number Theory, *History of Mathematics Sources* **16**, Amer. Math. Soc. & London Math. Soc., 1999. 7

[FT91] A. Fröhlich and M.J. Taylor, Algebraic Number Theory, Cambridge University Press, 1991. 2, 6

[GS98] J. von zur Gathen and I. E. Shparlinski, Orders of Gauss periods in finite fields, . *Appl. Algebra Engrg. Comm. Comput.* **9** (1998), no. 1, 15–24. 1

[GV95] S. Gao and S. A. Vanstone, On orders of optimal basis generators, *Math. Comp.* **64** (1995), no. 211, 1227–1233. 1, 8

[IK98] M. Ishikawa and Y. Kitaoka, On the distribution of units modulo prime ideals in real quadratic fields, *J. reine angew. Math.* **494** (1998), 65–72. 3

[Kat03] N. Kataoka, The distribution of prime ideals in a real quadratic field with units having a given index in the residue class field, *J. Number Theory* **101** (2003), no. 2, 349–375. 5

[Pop12] R. Popovych, Elements of high order in finite fields of the form $\mathbb{F}_q[x]/\Phi_r(x)$, *Finite Fields Appl.* **18** (2012), No. 4, 700–710. 1

[Pop14] R. Popovych, Sharpening of the explicit lower bounds for the order of elements in finite field extensions based on cyclotomic polynomials. *Ukrainian Math. J.* **66** (2014), no. 6, 916–927. 1

[SK67] D. Shanks and S. Kravitz, On the distribution of Mersenne divisors. *Math. Comp.* **21** (1967), 97–101. 9

[Ste96] P. Stevenhagen, On a problem of Eisenstein, *Acta Arith.* **74** (1996), no. 3, 259–268. 5

[Wag83] S.S. Wagstaff, Jr., Divisors of Mersenne Numbers, *Math. Comp.* **40** (1983), 385–397. 8

School of Mathematical and Physical Sciences, University of Newcastle, Newcastle,NSW 2308, Australia

Email address: florian.breuer@newcastle.edu.au