CLASS NUMBER PARITY FOR THE $p$TH CYCLOMATIC FIELD

PETER STEVENHAGEN

ABSTRACT. We study the parity of the class number of the $p$th cyclotomic field for $p$ prime. By analytic methods we derive a parity criterion in terms of polynomials over the field of 2 elements. The conjecture that the class number is odd for $p$ a prime of the form $2q+1$, with $q$ prime, is proved in special cases, and a heuristic argument is given in favor of the conjecture. An implementation of the criterion on a computer shows that no small counterexamples to the conjecture exist.

1. Introduction

In this paper, we will be interested in the parity of the class number $h_p$ of the $p$th cyclotomic field $\mathbb{Q}(\zeta_p)$ for $p$ a prime number. This question, and more generally the parity of abelian number fields, has been studied since Kummer introduced cyclotomic class numbers, and the literature on the subject is quite extensive. We refer to [4, 10] and the references given there for results on the parity of class numbers that will not be mentioned in the sequel.

We will not be concerned with general parity criteria for large classes of abelian fields as in [6, 7], but restrict ourselves to the special case of a cyclotomic field of prime conductor. This is the simplest example of a cyclotomic field, and it has a certain classical status ever since Kummer introduced the theory of ideal factorization for it that became the basis of algebraic number theory. Moreover, it turns out that the parity problem is the hardest for this field, since many criteria for the class number to be even, like those of Cornell and Rosen [2] that we will discuss momentarily, only apply to fields of composite conductor.

We will derive a parity criterion for $h_p$ in the spirit of [3] and [5] in the case that $p$ is a so-called Sophie Germain prime. This makes for easy calculation, both on a theoretical level, where we will show how it leads to elementary proofs of the known results, most notably the main result of [4], and on a computational level, where we will deal with primes $p$ that are “small” in a special sense. We also develop a heuristic argument that shows very convincingly that we should not expect any Sophie Germain prime $p$ to exist for which $h_p$ is even.

We introduce some notation in order to describe our results in more detail.

For $n \geq 1$ an integer, let $\text{Cl}_n$ denote the class group of $\mathbb{Q}(\zeta_n)$ and $\text{Cl}_n^+$ the class group of the real subfield $\mathbb{Q}(\zeta_n)^+$. It is known that the natural map $\text{Cl}_n^+ \to \text{Cl}_n$ is injective and that the norm map $N_n: \text{Cl}_n \to \text{Cl}_n^+$ is surjective [9, pp. 82–84]. Correspondingly, we have a decomposition $h_n = h_n^- h_n^+$, where
$h^+_n$ denotes the order of $\text{Cl}_n^+$ and $h^-_n$ the order of $\ker N_n$. The intersection $\text{Cl}_n^+ \cap \ker N_n$ is the 2-torsion subgroup $\text{Cl}_n^+ [2]$ of $\text{Cl}_n^+$, and one sees that

$$2|h^+_n \Rightarrow 2|h^-_n.$$ 

It follows that the parity of $h_n$ can be determined by looking at $h^-_n$ only.

The number $h^+_n$ is not easily computed, but its parity can be determined without a computation of the number itself. It has been shown by Cornell and Rosen [2] that $h^+_n$ is even when $n$ is divisible by five or more primes, and they give an explicit lower bound on the 2-rank of $\text{Cl}_n^+$ that tends to infinity with the number of primes dividing $n$. When $n$ is divisible by two, three, or four primes, they prove parity results for $h^+_n$ and $h_n$ under additional assumptions on these primes. However, in the case that $n = p$ is prime, which is the situation we will consider in the present paper, the methods of [2] do not yield anything. It is known that the class numbers $h^+_p$ and $h_p$ can be either even or odd. The smallest value of $p$ for which $h^+_p$ is even is $p = 29$, and the smallest value for which $h^-_p$ is even is $p = 163$.

We deal with the following conjecture concerning the parity of $h_p$ for Sophie Germain primes $p$, i.e., primes $p$ for which $q = (p - 1)/2$ is prime. Note that the terminology is somewhat questionable as the prime of interest in the Sophie Germain criterion for the first case of Fermat's last theorem is $q$ rather than $p$. The conjecture seems to have arisen in connection with work of Taussky [11], even though it is stated explicitly only in a paper of Davis [3]. More details on its history can be found in the introduction of [4]. A formulation of the conjecture in terms of the $K_2$-group of the ring of integers of the real cyclotomic field can be found in [8].

1.2. Conjecture. If $p$ is a Sophie Germain prime, then $h_p$ is odd.

It has not been proved that the number of Sophie Germain primes is infinite, but this is what one expects. The heuristic argument in [1] can be applied in our special case to estimate the number $P(N)$ of positive integers $x < N$ for which both $x$ and $2x + 1$ are prime, and it leads to

$$P(N) \sim C \int_2^N \frac{dt}{\log^2 t} \quad \text{for } N \to \infty,$$

where the constant $C$ is defined by

$$C = 2 \prod_{p > 2 \text{ prime}} \left(1 - \frac{1}{(p - 1)^2}\right).$$

This constant is known as the twin prime constant because exactly the same heuristics apply to the case of twin primes, in which one looks at primes $x$ for which $x + 2$ is also prime. The numerical value of $C$ is close to 1.32032. These heuristics are in reasonable accordance with numerical observations, as Table 1 shows. In any case, we can feel confident that the number $P(N)$ does tend to infinity with $N$.

In this paper, we will derive the following criterion for the parity of $h_p$ for $p$ a Sophie Germain prime.
1.3. **Theorem.** Let \( q > 2 \) and \( p = 2q + 1 \) be prime numbers, and denote by \( \phi \) some isomorphism \((\mathbb{Z}/p\mathbb{Z})^*/(-1) \sim \mathbb{Z}/q\mathbb{Z}\). Then the polynomial \( F_q = \sum_{i=1}^{(p-3)/4} X^{\phi(i)} \in \mathbb{F}_2[X] \) is well defined modulo the cyclotomic polynomial \( \Phi_q = (X^q - 1)/(X - 1) \), and one has

\[
h_q \text{ is odd } \Rightarrow \text{gcd}(F_q, \Phi_q) = 1 \in \mathbb{F}_2[X].
\]

We will see in §2 how this criterion can be used to prove Conjecture 1.2 for special classes of \( p \), and in our final §3 we will apply it to furnish a heuristic argument that shows that counterexamples to Conjecture 1.2 are highly unlikely to occur. More precisely, we show that under the assumption that the polynomial \( F_q \) behaves like a random element in \( \mathbb{F}_2[X]/\Phi_q \), the expected number of counterexamples to 1.2 is finite and very small. Some numerical data are presented to show that counterexamples that are small in a sense to be defined do not exist. For instance, one obtains the following theorem that excludes the existence of small values of \( p \) contradicting 1.2.

1.4. **Theorem.** Suppose that \( p \) is a Sophie Germain prime for which \( h_p \) is even. Then \( h_p \) is divisible by \( 2^{95} \).

The exponent 95 can be replaced by a higher value \( M \) if the gcd in Criterion 1.3 is found to be equal to 1 for the finite number of Sophie Germain primes \( q = 2p + 1 \) for which the multiplicative order of 2 modulo \( p \) is bounded by \( M \). For instance, the exponent can be replaced by 100 after the verification of the single case \( p = 841557503 \). We obtained the exponent 95 by checking the criterion on a computer for 19 values of \( p \) that are listed in Table 4.3 at the end of §3.

### Table 1

<table>
<thead>
<tr>
<th>( N )</th>
<th>( \frac{C}{2} \int_2^N \frac{dt}{\log^2(t)} )</th>
<th>( P(N) )</th>
</tr>
</thead>
<tbody>
<tr>
<td>100000</td>
<td>1248.4</td>
<td>1171</td>
</tr>
<tr>
<td>200000</td>
<td>2181.4</td>
<td>2058</td>
</tr>
<tr>
<td>300000</td>
<td>3037.0</td>
<td>2848</td>
</tr>
<tr>
<td>400000</td>
<td>3847.6</td>
<td>3589</td>
</tr>
<tr>
<td>500000</td>
<td>4626.9</td>
<td>4324</td>
</tr>
<tr>
<td>1000000</td>
<td>8246.0</td>
<td>7746</td>
</tr>
</tbody>
</table>

2. **The parity criterion**

We will now give the proof of Theorem 1.3, which is based on the analytic class number formula for relative class numbers [9, Theorem 3.2]. It states that for a totally complex abelian extension \( K \) of \( \mathbb{Q} \) with maximal real subfield \( K^+ \), the relative class number \( h_K^- = h_K/h_{K^+} \) can be written as

\[
h_K^- = Q_K w_K \prod_\chi (-\frac{1}{2} B_{1,\chi}),
\]

where \( w_K \) is the order of the group \( Z_K \) of roots of unity in \( K \) and \( Q_K = [E_K : Z_K E_{K^+}] \in \{1, 2\} \) is the unit index. The product ranges over all odd characters \( \chi : \text{Gal}(K/\mathbb{Q}) \to \mathbb{C}^* \), and \( B_{1,\chi} \) is a generalized Bernoulli number.
Proof of 1.3. We apply (2.1) with $K = \mathbb{Q}(\zeta_p)$ and note that the Bernoulli number corresponding to the quadratic character $\chi = (\overline{\cdot}^p)$ is, again by (2.1), equal to minus the class number of the quadratic subfield $\mathbb{Q}(\sqrt{-p})$. It is an easily verified and well-known fact that this class number is odd. Using the implication (1.1), we see that $h_p$ is odd if and only if the integer $h^* = h_p/\mathcal{N}_{\mathbb{Q}(\zeta_p)/\mathbb{Q}}$ is. Apart from the quadratic character, all odd characters modulo $p$ have order $2q$, and they are transitively permuted by the Galois group of $\mathbb{Q}(\zeta_q)/\mathbb{Q}$ that acts naturally on their image. We obtain

$$h^* = \frac{\mathcal{N}_{\mathbb{Q}(\zeta_p)/\mathbb{Q}}}{\mathcal{N}_{\mathbb{Q}(\sqrt{-p})/\mathbb{Q}}} \prod_{\text{ord}(\chi) = 2q} \left\{ \frac{-1}{2p} \sum_{x=1}^{2q} x\chi(x) \right\}\left( \frac{1}{2} \sum_{x=1}^{2q} x\chi(x) \right).$$

In the last expression, we can take any fixed character $\chi$ modulo $p$ of order $2q$. It follows that $h^*$ is odd if and only if for this $\chi$ the element $w_\chi = \frac{1}{2} \sum_{x=1}^{2q} x\chi(x) \in \mathbb{Z}[\zeta_q]$ is odd; i.e., if its residue class in $\mathbb{Z}[\zeta_q]/2\mathbb{Z}[\zeta_q]$ is a unit.

In order to determine whether $w_\chi$ is odd, we may replace it by $mw_\chi$ for any odd multiplier $m \in \mathbb{Z}[\zeta_q]$. As $\chi(2)$ is a root of unity of order $q$ or $2q$, we can take $m = \overline{x}(2) - 1$ and use the substitution $x \mapsto 2x - p[2x/p]$ for $x = 1, 2, \ldots, 2q = p - 1$ to obtain

$$mw_\chi = (\overline{x}(2) - 1) \frac{1}{2} \sum_{x=1}^{2q} x\chi(x) = \sum_{x=1}^{2q} (x/2)\chi(x/2) - \frac{1}{2} \sum_{x=1}^{2q} x\chi(x)$$

$$= \frac{1}{2} \sum_{x=1}^{2q} x\chi(x) - \frac{1}{2} \sum_{x=q+1}^{2q} \chi(x)$$

$$= \frac{1}{2} \sum_{x=1}^{q} \{x\chi(x) + (p - x)\chi(p - x)\} + \frac{1}{2} p \sum_{x=1}^{q} \chi(x)$$

$$= \sum_{x=1}^{q} x\chi(x) + \frac{1}{2} p \sum_{x=1}^{q} \chi(-x) + \chi(x) = \sum_{x=1}^{q} x\chi(x).$$

Modulo the ideal $(2) \subset \mathbb{Z}[\zeta_q]$, the character $\chi$ coincides with the even character $\psi = \chi \cdot (\overline{\cdot}^p)$, and using the identity $\sum_{x=1}^{q} \psi(x) = 0$, we obtain

$$mw_\chi = \sum_{x=1}^{q} x\chi(x) \mod 2 \sum_{x=1}^{q} \psi(x) = \sum_{x=1}^{q} \psi(x) = \psi(2) \sum_{x=1}^{(q-1)/2} \psi(x).$$

We conclude that $h_p^*$ is odd if and only if $\sum_{x=1}^{(q-1)/2} \psi(x)$ is odd in $\mathbb{Z}[\zeta_q]$. We can write $\mathbb{Z}[\zeta_q]/2\mathbb{Z}[\zeta_q] \cong \mathbb{F}_2[X]/\Phi_q(X)$, and choosing $\phi$ as stated in the theorem, we have $\psi(x) = \phi\overline{x}^{(q-1)/2}$ for some choice of the root of unity $\zeta_q$. Obviously, an element $\sum a_i\zeta_q^i$ is a unit in $\mathbb{Z}[\zeta_q]/2\mathbb{Z}[\zeta_q]$ if and only if the polynomial $\sum a_iX^i$ is coprime to $\Phi_q$ in $\mathbb{F}_2[X]$. The theorem follows. □

2.2. Remark. One can use multipliers different from $m = \overline{x}(2) - 1$ in the preceding proof to obtain versions of Theorem 1.3 in which other polynomials

License or copyright restrictions may apply to redistribution; see http://www.ams.org/journal-terms-of-use
play the role of $F_q$. For instance, it is immediate from equation (*) in the preceding proof that the choice $m = \overline{\chi}(2) - 2$ leads to $m \psi(x) = \frac{1}{p} \sum_{x=1}^{q} \chi(x)$. Adding $\frac{1}{p} \sum_{x=1}^{q} \psi(x) = 0$ to this element, it follows that we may replace $F_q$ in Theorem 1.3 by

$$F'_q = \sum_{x=1}^{q} X^\phi(x).$$

As a direct consequence of the Criterion 1.3, we see that Conjecture 1.2 holds for the following class of Sophie Germain primes. This result appears already in [3].

2.3. **Corollary.** Suppose that $p = 2q + 1$ is a Sophie Germain prime such that 2 is a primitive root modulo $q$. Then $h_p$ is odd.

**Proof.** Under the assumption, $\Phi_q$ is irreducible in $F_2[X]$, so the greatest common divisor in the criterion must be 1. □

The proof of Theorem 1.3 describes the factor $h^*$ of $h_p^*$ as the norm of an element in $Z[\zeta_q]$. If this norm is even, it is obviously divisible by $2^{f(q)}$, where $f(q)$ is the residue class degree of the primes over 2 in $Q(\zeta_q)$, i.e., the order of 2 mod $q$ in $F_q^*$. We have obtained the following corollary.

2.4. **Corollary.** Suppose $p = 2q + 1$ is a Sophie Germain prime for which $h_p$ is even. Then $h_p^*$ is divisible by $2^{f(q)}$, where $f(q)$ is the multiplicative order of 2 modulo $q$.

We will now use Theorem 1.3 to prove Conjecture 1.2 for a class of primes that fails to meet the conditions of Corollary 2.3, but is still "sufficiently close" to these conditions. This result is due to Estes [4], who gave a rather involved proof that makes extensive use of the properties of Dedekind sums. Our proof is somewhat similar in the sense that it also points out a nonzero coefficient in a certain polynomial, but it is completely elementary.

2.5. **Theorem.** Let $p = 2q + 1$ be a Sophie Germain prime with $q \equiv 3$ mod 4, and suppose that $2 \mod q$ generates the subgroup of squares in $F_q^*$. Then $h_p$ is odd.

**Proof.** Under our hypothesis on $q$, the group $F_q^*$ is generated by 2 and $-1$. The cyclotomic polynomial $\Phi_q$ then factors over $F_2[X]$ as the product of an irreducible polynomial of degree $(q-1)/2$ and the reciprocal of this polynomial. We have to verify that the polynomial $F_q$ from 1.3 is not divisible by one of these factors in $F_2[X]/\Phi_q(X)$, or, equivalently, that we have the relation $G(X) \equiv F_q(X)F_q(X^{-1}) \neq 0 \in F_2[X]/\Phi_q(X)$. We can write $G$ explicitly as

$$G = \sum_{z=1}^{(p-3)/2} c(z, p)X^{\phi(z)}$$

with coefficients given by

$$c(z, p) = \#\{(x, y) : 1 \leq x, y < p/4 \text{ and } x \equiv \pm yz \mod p\} \mod 2,$$

and we have to show that the coefficients $c(z, p)$ do not all have the same parity. This is true in the following generality.

2.7. **Lemma.** Let $p \equiv 3 \mod 4$ be an arbitrary prime number, and define the numbers $c(z, p) \in \mathbb{Z}/2\mathbb{Z}$ for $z = 1, 2, \ldots, p-1$ by (2.6). Then these numbers are not all equal.
Proof. In order to compute the numbers \( c(z, p) \), we have to count how many of the numbers \( yz \), with \( 1 \leq y < p/4 \), lie in an interval of the form \((kp - p/4, kp + p/4) = ((4k - 1)p/4, (4k + 1)p/4)\) with \( k \in \mathbb{Z} \). Using square brackets to denote the integer function, we can write the number of multiples of an integer \( z \) in an interval \((a, b)\) with \( a \) and \( b \) not integral multiples of \( z \) as \( [b/z] - [a/z] = [a/z] + [b/z] \mod 2 \). Setting \( l = [z/4] \), we can thus express \( c(z, p) \) as

\[
c(z, p) = \begin{cases} 
\sum_{i=0}^{2l} \left\lfloor \frac{(2i+1)p}{4z} \right\rfloor \mod 2 & \text{if } 4 \nmid z, \\
\sum_{i=0}^{2l-1} \left\lfloor \frac{(2i+1)p}{4z} \right\rfloor + \left\lfloor \frac{p}{4} \right\rfloor \mod 2 & \text{if } 4 | z.
\end{cases}
\]

(In case \( z = 4l \), the largest \( z \)-multiple \( \lfloor \frac{z}{4} \rfloor \) lies in the interval \(( (4l - 1)p/4, (4l + 1)p/4 ) \), so our last endpoint has to be taken as \( z/2 \).)

This formula makes sense for any pair of nonzero integers, and it shows that apart from the obvious relation \( c(z_1, p) = c(z_2, p) \) for \( z_1 \equiv z_2 \mod p \) we also have \( c(z, p_1) = c(z, p_2) \) whenever \( p_1 \equiv p_2 \mod 8z \). If \( 4 | z \), the last conclusion already holds when we have \( p_1 \equiv p_2 \mod 4z \). If \( a \) and \( b \) are coprime to \( p \) and \( z = ab^{-1} \in (\mathbb{Z}/p\mathbb{Z})^* \), we write \( c(a/b, p) \) for \( c(z, p) \). In this case there is a similar argument showing that \( c(a/b, p_1) = c(a/b, p_2) \) when \( p_2 \equiv p_1 \mod 8ab \) (or \( p_2 \equiv p_2 \mod 4ab \) when \( ab \) is even).

We have \( c(1, p) = \lfloor \frac{p}{2} \rfloor \) and \( c(2, p) = \lfloor \frac{p}{3} \rfloor \), so the first two coefficients are both \( 0 \in \mathbb{Z}/2\mathbb{Z} \) if \( p \equiv 3 \mod 16 \) and both \( 1 \in \mathbb{Z}/2\mathbb{Z} \) when \( p \equiv -1 \mod 16 \). In other cases they have different parity and we are done.

Assume first that \( p \equiv 3 \mod 16 \), and write \( p = u2^m + 3 \) with \( u \) odd and \( m \geq 4 \). We claim that \( c(z, p) = 1 \) for \( z = 2^{m-1} \). Indeed, we have \( 4 | z \) and \( p \equiv 2^m + 3 \mod 4z \), so \( c(2^{m-1}, p) = c(2^{m-1}, 2^m + 3) = c(-3/2, 2^m + 3) \). The value of the last symbol only depends on the residue class of \( 2^m + 3 \) modulo \( 8 \cdot 3 \cdot 2 = 48 \), which is either \( 19 \) or \( 35 \) mod \( 48 \) depending on the parity of \( m \). In either case we find \( c(z, p) = 1 \) as \( c(-3/2, 35) = c(11, 35) = 1 \) and \( c(-3/2, 19) = c(7, 19) = 1 \).

Assume now that \( p \equiv -1 \mod 16 \). In this case we want an element \( c(z, p) = 0 \), and this time no power of 2 seems to work for \( z \). We can however work with powers of 3, a phenomenon that already occurs in Estes's proof of this result. Observe first that \( c(3, p) = \lfloor \frac{p}{2} \rfloor \), so \( c(3, p) = 0 \) when \( p \equiv 31 \mod 48 \). We may therefore assume that \( p \equiv -1 \mod 48 \). Write \( p = u \cdot 3^m - 1 \) with \( u \) divisible by \( 16 \) but not by \( 3 \) and \( m \geq 1 \). We claim that \( c(z, p) = 0 \) for \( z = 2 \cdot 3^{m+1} \). This time \( p \mod 8z = 2^33^{m+1} \) depends on \( u \mod 3 \), so we distinguish two cases.

If \( u \equiv 1 \mod 3 \), we have \( c(2 \cdot 3^{m+1}, p) = c(2 \cdot 3^{m+1}, 16 \cdot 3^m - 1) = c(3/8, 16 \cdot 3^{m+1} - 1) \). This reduces for odd \( m \) to \( c(3/8, 47) = c(13, 47) = 0 \) and for even \( m \) to \( c(3/8, 143) = c(45, 143) = 0 \).

If \( u \equiv -1 \mod 3 \), we have \( c(2 \cdot 3^{m+1}, p) = c(2 \cdot 3^{m+1}, 32 \cdot 3^m - 1) = c(3/16, 32 \cdot 3^{m+1} - 1) \). This reduces for odd \( m \) to \( c(3/16, 95) = c(18, 95) = 0 \) and for even \( m \) to \( c(3/16, 287) = c(54, 287) = 0 \). This finishes the proof of Lemma 2.7 and of Theorem 2.5. □
Criteria in the spirit of our Theorem 1.3 can also be derived by studying the signatures of the cyclotomic units in $Q(\zeta_p)$. One uses the analytic fact that $h_p^+$ is the index of the group of cyclotomic units in the full unit group of $Q[\zeta_p]$ and works inside the real cyclotomic field $Q(\zeta_p)^+$. We will indicate this approach, which is more common in the literature [3, 4, 5, 6, 7] in the rest of this section and compare the results obtained to ours.

For parity questions, one has first of all the following equivalences.

2.8. **Lemma.** The following are equivalent for a prime number $p$:

(i) $h_p$ is odd;

(ii) $h_p^-$ is odd;

(iii) $h_{p,\text{narrow}}^+$ is odd.

Proof. The equivalence (i) \(\Leftrightarrow\) (ii) follows from implication (1.1) in the introduction.

For (i) \(\Leftrightarrow\) (iii) we use arguments as in 2.1. As any abelian extension $F/Q(\zeta_p)^+$ that is unramified at all finite primes and of even degree gives rise to an unramified extension $F(\zeta_p)/Q(\zeta_p)$ that is totally unramified of the same degree, we see that $h_{p,\text{narrow}}^+$ divides $h_p$, so $h_p$ is even if $h_{p,\text{narrow}}^+$ is even. Conversely, if $h_p$ is even there is an unramified abelian extension $F/Q(\zeta_p)$ of 2-power degree such that $F/Q(\zeta_p)^+$ is Galois, say with group $H$. Let $I \subset H$ be an inertia group of a prime of $F$ lying over $p$. As the 2-group $H$ is solvable, it has a normal subgroup $N$ of index 2 that contains the subgroup $I$ of order 2. The fixed field of $N$ is a quadratic extension of $Q(\zeta_p)^+$ that is unramified at all finite primes, so it follows that $h_{p,\text{narrow}}^+$ is even. \(\square\)

The last condition in the preceding lemma gives rise to parity conditions in terms of cyclotomic units. We need some additional notation in order to state them.

Let $E$ be the unit group of the ring of integers $Q(\zeta_p)^+$. Then $Q(\zeta_p) \cdot E$ is the unit group in $Q(\zeta_p)$, and we call a unit in this group cyclotomic if it is in the subgroup of $Q(\zeta_p)^*$ generated by $\zeta_p$ and the nonzero elements of the form $1 - \zeta_p^i$. The group of cyclotomic units is generated by $\zeta_p$ and the group $C$ of real cyclotomic units. As abelian groups, both $E$ and $C$ can be written as the product of their torsion subgroup $(-1)$ and a free abelian group on $q - 1$ generators, with $q = (p - 1)/2$ the degree of $Q(\zeta_p)^+$ over $Q$. The analytic class number formula for $Q(\zeta_p)^+$ states [9, Theorem 5.1] that the index $[E : C]$ is equal to the class number $h_p^+$. In order to study the parity of $h_p^+ = \#(E/C)$, we define a signature map on $Q(\zeta_p)^+$ that respects the action of $G = \text{Gal}(Q(\zeta_p)^+/Q)$. Let $\text{sgn} : R^+ \to F_2$ be the signature map with values in the additive group $F_2$ rather than in $(-1)$. From now on, we fix an embedding $Q(\zeta_p) \subset C$ by taking $\zeta_p = e^{2\pi i/p}$. Then $\text{sgn}(x) \in F_2$ is well defined for any nonzero $x \in Q(\zeta_p)^+$, and we have the $G$-homomorphism

$$S : (Q(\zeta_p)^+)^* \to F_2[G]$$

$$x \mapsto \sum_{g \in G} \text{sgn}(g^{-1}(x)) \cdot g.$$

For parity questions, one studies the values of $S$ on $E$ and $C$. From the structure of the abelian group $E$ one sees that the signature map $S : E \to F_2[G]$
Peter Stevenhagen is surjective if and only if the subgroup $E^+ = \ker S|_E$ of totally positive units coincides with the subgroup $E^2$ of squares in $E$. An analogous remark applies to the group $C$.

2.9. Lemma. Let $p$ be a prime number. Then $h_p$ is odd if and only if $S$ maps the group of real cyclotomic units $C$ surjectively to the signature space $\mathbb{F}_2[G]$.

Proof. By the preceding lemma, $h_p$ is odd if and only if $h^+_p,\text{narrow}$ is odd. As $h^+_p,\text{narrow} = [F_2[G] : S[E]] \cdot h^+_p$, we conclude that $h_p$ is odd if and only if $S[E] = F_2[G]$ and $h^+_p = [E : C]$ is odd. If these two conditions are satisfied, then $S[C] = S[E] = F_2[G]$ because the index $[S[E] : S[C]]$ is odd and divides $|F_2[G]| = 2^q$. Conversely, if $S[C] = F_2[G]$, then we have $S[E] = F_2[G]$ and $E = C \cdot \ker S|_E = CE^2$, which implies that the order $h^+_p$ of $E/C$ is odd. □

The subspace $S[C] \subset F_2[G]$ can be described explicitly, as we know $C$ explicitly. Let $\sigma$ denote a generator of $G$, and set $\eta_i = (\zeta_p - \zeta_p^{-1})^{(i-1)}$ for $i \in \mathbb{Z}$. Note that $\eta_q = -1$ and that $\eta_{i+q} = -\eta_i$. The group $C$ is generated by the elements $\eta_i$ with $i = 1, 2, \ldots, q$. From the relation $\eta_{i+k} = \sigma^k(\eta_i)$ it follows inductively that $\eta_1$ generates $C/(1)$ over the group ring. As $S$ maps $-1$ to $N_G = \sum_{g \in G} g$, we have an induced homomorphism between cyclic $F_2[G]$-modules:

$$\overline{S}: C = C/(1) \to F_2[G]/N_G \cong F_2[X]/\Phi_q(X).$$

Under the last isomorphism, the generator $\sigma$ of $G$ corresponds to $X$. The image of $C$ in $F_2[X]/\Phi_q(X)$ is the ideal generated by $\overline{S}(\eta_1)$, so the class number $h_p$ is odd if and only if $\overline{S}(\eta_1)$ is a unit in $F_2[X]/\Phi_q(X)$.

We have obtained a criterion analogous to our Theorem 1.3. It immediately yields 2.3 by observing that $\overline{S}$ is not the zero map for $p > 3$—it suffices to note that $\zeta_p + \zeta_p^{-1}$ cannot be in the kernel—and also 2.4 with $h^\pm_p$ replaced by $h_p$.

One can give $\overline{S}(\eta_1)$ explicitly as a polynomial. An element $s_1 \in G$ acts on $\overline{\eta}_1 = \eta_1/\eta_0$ by shifting the indices over $i$ places. Writing $s_1 = \text{sgn}(\eta_{i-1}) \in F_2$ and $H = \sum_{i=0}^{q-1} s_1 X^i$, we obtain $\text{sgn}(\sigma^{-i}(\eta_1)) = s_{i-1} + s_i$ and therefore

$$\overline{S}(\eta_1) = \sum_{i=1}^{q} (s_{i-1} + s_i)X^i = S_q X^q + (X + 1) \sum_{i=0}^{q-1} s_i X^i + s_0 = 1 + (X + 1)H(X) \in F_2[X]/\Phi_q.$$
3. Heuristics

In this section we will show that under certain assumptions of randomness, the number of Sophie Germain primes for which \( h_p \) is even is a finite number whose expected value is very close to zero.

As before, we denote for a Sophie Germain prime \( p > 5 \) the prime number \((p-1)/2\) by \( q \). Let \( f(q) \) be the order of \( 2 \) in the multiplicative group \((\mathbb{Z}/q\mathbb{Z})^*\). Our parity Criterion 1.3 states that \( h_p \) is even if and only if the element \( F_q \) is not a unit in the finite algebra

\[
\mathbb{F}_2[X]/\Phi_q(X) \cong (\mathbb{F}_2/(q^f))^{(q-1)/f(q)}.
\]

A random element in this algebra is a nonunit with probability

\[
\pi(q) = 1 - \left(1 - 2^{-f(q)}\right)^{(q-1)/f(q)}.
\]

Since we are unable to prove very much about \( F_q \), we will base our heuristic analysis on the assumption that \( F_q \) behaves like a random element in \( \mathbb{F}_2[X]/\Phi_q(X) \) when \( q \) ranges over the primes \( q > 2 \) for which \( p = 2q + 1 \) is prime. Under this assumption, we expect \( \sum_q \pi(q) \) Sophie Germain primes \( p \) for which \( h_p \) is even. We prove the following result.

3.1. Theorem. The sum \( \sum_q \pi(q) \) over all primes \( q > 2 \) for which \( 2q + 1 \) is prime is finite.

Proof. From the inequality \( \left(1 - 2^{-f}\right)^{(q-1)/f} \geq 1 - (q-1)/(2^f) \) it follows that the terms of our sum satisfy

\[
\pi(q) = 1 - \left(1 - 2^{-f(q)}\right)^{(q-1)/f(q)} \leq \frac{q-1}{f(q)2^{f(q)}}.
\]

Ordering the values of \( q \) over which the sum is taken by the size of the corresponding value of \( f(q) \), we rewrite the sum as

\[
\sum_{f=2}^{\infty} w_f \quad \text{with} \quad w_f = \sum_{q: f(q)=f} \pi(q),
\]

with \( q \) ranging over the odd primes for which \( 2q + 1 \) is prime, and estimate each of the terms \( w_f \).

For given \( f \), all primes \( q \) with \( f(q) = f \) are divisors of \( 2^f - 1 \), so the number of such \( q \) cannot exceed \( f \). For the primes \( q \) that satisfy \( q < 2^{f/2} \) one has

\[
\pi(q) \leq \frac{q-1}{f2^f} \leq \frac{1}{f2^{f/2}},
\]

so the contribution of these \( q \) of \( w_f \) does not exceed \( 2^{-f/2} \). If \( 2^f - 1 \) has a prime divisor \( q > 2^{f/2} \), then this prime divisor is obviously unique. For such \( q \), we will obtain two different estimates for \( \pi(q) \), depending on whether \( f \) is prime or composite.

If \( f \) is composite, it has a divisor \( d \geq \sqrt{f} \), and the definition of \( f(q) \) shows that \( q \) divides \( (2^f - 1)/(2^d - 1) \leq (2^f - 1)/(2\sqrt{f} - 1) \), so in this case
we have
\[ \pi(q) \leq \frac{q - 1}{f^{2f}} < \frac{1}{f(2\sqrt{f} - 1)}. \]

If \( f > 2 \) is prime, then \( q \neq 2f - 1 \) for the \( q \) that contribute to \( w_f \), as equality would imply that \( p = 2q + 1 \equiv 0 \mod 3 \). All prime factors of \( 2^f - 1 \) are congruent to 1 mod \( f \), so they are bounded from below by \( 2f + 1 \). It follows that \( q \leq (2f - 1)/(2f + 1) \), and consequently
\[ \pi(q) \leq \frac{q - 1}{f^{2f}} < \frac{1}{2f^2}. \]

We conclude that
\[ (3.2) \quad w_f < \frac{1}{2f^2} + \frac{1}{f(2\sqrt{f} - 1)} + \frac{1}{2f^2} \]
for every \( f > 2 \). In particular, we obtain a convergent sum when summing over \( f \). \( \Box \)

Our heuristic approach suggests that counterexamples to Conjecture 1.2, if they exist, should be found for small values of \( f(q) \) rather than for small values of \( q \) itself. Table 3.3 lists all values \( q > 2 \) for which \( p = 2q + 1 \) is prime and \( f(q) \leq 100 \). In the column “\( h_p \) odd?” we list 2.3 and 2.5 if the class number is odd, because the hypotheses for these theorems are satisfied. For the remaining 20 values of \( p \) we have attempted the numerical verification of the criterion given in Theorem 1.3. For the 12 values of \( p \) below 2500 this could be done on the Pari-calculator, and these cases have been marked \( P \). All other primes in the table except for the largest prime \( p = 841557503 \) were dealt with by Bert Ruitenburg, who used Maple (M) in six cases and a special-purpose C-program for \( p = 26529059 \).

In the larger cases one can reduce the time needed for the computation by running the algorithm on parallel machines. This is due to the fact that one knows in principle how the cyclotomic polynomial \( \Phi_q \) factors over the field \( \mathbf{F}_2 \). Thus, once one has computed the polynomial \( F_q \) in 1.3, one can check the criterion by verifying that \( F_q \) does not vanish on any primitive \( q \)th root of unity in \( \mathbf{F}_{2^f} \). It is easy to find one such root of unity \( \zeta_p \) once one has “constructed” \( F_{2^f(q)} \) by exhibiting an irreducible polynomial of degree \( f(q) \) over \( \mathbf{F}_2 \). The algorithm then reduces to \( (q - 1)/f(q) \) independent verifications showing that \( F_q(\zeta_p^a) \neq 0 \) for all \( a \in (\mathbb{Z}/q\mathbb{Z})^*/(2) \), so it is easily run in parallel.

Combining the results in the table with Corollary 2.4, we immediately obtain a proof of Theorem 1.4 stated in the introduction. It is also clear that the exponent in this theorem can be increased by extending the range of our table and performing the necessary computations.

As another consequence of our numerical work, we can bound the number of expected counterexamples to Conjecture 1.2 rather drastically by considering in the sum \( \sum_q \pi(q) \) from Theorem 3.1 only those \( q \) for which \( f(q) \geq 95 \). Using the rough estimate from (3.2), one expects to find at most \( \sum_{f \geq 95} w_f < .01 \) counterexamples. As Table 3.3 already suggests, the exact value of this sum is much smaller than .01. This heuristic argument convinces us that Conjecture 1.2 must be true “for lack of counterexamples”.

License or copyright restrictions may apply to redistribution; see http://www.ams.org/journal-terms-of-use
3.3. Table. Sophie Germain primes $p = 2q + 1$ with $f(q) \leq 100$

<table>
<thead>
<tr>
<th>$f(q)$</th>
<th>$q$</th>
<th>$p$</th>
<th>$\pi(q)$</th>
<th>$h_p$ odd?</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>3</td>
<td>7</td>
<td>.25</td>
<td>2.3</td>
</tr>
<tr>
<td>4</td>
<td>5</td>
<td>11</td>
<td>.0625</td>
<td>2.3</td>
</tr>
<tr>
<td>10</td>
<td>11</td>
<td>23</td>
<td>.009765625</td>
<td>2.3</td>
</tr>
<tr>
<td>11</td>
<td>23</td>
<td>47</td>
<td>.009763241</td>
<td>2.5</td>
</tr>
<tr>
<td>89</td>
<td>179</td>
<td>.0038995808</td>
<td>P</td>
<td></td>
</tr>
<tr>
<td>20</td>
<td>41</td>
<td>83</td>
<td>.000019073</td>
<td>P</td>
</tr>
<tr>
<td>22</td>
<td>683</td>
<td>1367</td>
<td>.0000073909</td>
<td>P</td>
</tr>
<tr>
<td>28</td>
<td>29</td>
<td>59</td>
<td>.37253 E − 8</td>
<td>2.3</td>
</tr>
<tr>
<td>113</td>
<td>227</td>
<td>.14901 E − 7</td>
<td>P</td>
<td></td>
</tr>
<tr>
<td>29</td>
<td>233</td>
<td>467</td>
<td>.14901 E − 7</td>
<td>P</td>
</tr>
<tr>
<td>1103</td>
<td>2207</td>
<td>.70781 E − 7</td>
<td>P</td>
<td></td>
</tr>
<tr>
<td>34</td>
<td>43691</td>
<td>87383</td>
<td>.74797 E − 7</td>
<td>M</td>
</tr>
<tr>
<td>43</td>
<td>431</td>
<td>863</td>
<td>.11369 E − 11</td>
<td>P</td>
</tr>
<tr>
<td>46</td>
<td>2796203</td>
<td>5592407</td>
<td>.86384 E − 9</td>
<td>M</td>
</tr>
<tr>
<td>47</td>
<td>2351</td>
<td>4703</td>
<td>.35527 E − 12</td>
<td>P</td>
</tr>
<tr>
<td></td>
<td>13264529</td>
<td>26529059</td>
<td>.20053 E − 8</td>
<td>C</td>
</tr>
<tr>
<td>52</td>
<td>53</td>
<td>107</td>
<td>.22204 E − 15</td>
<td>2.3</td>
</tr>
<tr>
<td>53</td>
<td>69431</td>
<td>138863</td>
<td>.14544 E − 12</td>
<td>M</td>
</tr>
<tr>
<td>58</td>
<td>59</td>
<td>119</td>
<td>.34694 E − 17</td>
<td>2.3</td>
</tr>
<tr>
<td>64</td>
<td>641</td>
<td>1283</td>
<td>.54210 E − 18</td>
<td>P</td>
</tr>
<tr>
<td>68</td>
<td>953</td>
<td>1907</td>
<td>.47434 E − 19</td>
<td>P</td>
</tr>
<tr>
<td>70</td>
<td>281</td>
<td>563</td>
<td>.33881 E − 20</td>
<td>P</td>
</tr>
<tr>
<td></td>
<td>86171</td>
<td>172343</td>
<td>.10427 E − 17</td>
<td>M</td>
</tr>
<tr>
<td>71</td>
<td>228479</td>
<td>456959</td>
<td>.13629 E − 17</td>
<td>M</td>
</tr>
<tr>
<td>82</td>
<td>83</td>
<td>167</td>
<td>.20680 E − 24</td>
<td>2.3</td>
</tr>
<tr>
<td>92</td>
<td>1013</td>
<td>2027</td>
<td>.22214 E − 26</td>
<td>P</td>
</tr>
<tr>
<td></td>
<td>30269</td>
<td>60539</td>
<td>.66441 E − 25</td>
<td>M</td>
</tr>
<tr>
<td>95</td>
<td>191</td>
<td>383</td>
<td>.50487 E − 28</td>
<td>2.5</td>
</tr>
<tr>
<td></td>
<td>420778751</td>
<td>841557503</td>
<td>.11181 E − 21</td>
<td>?</td>
</tr>
</tbody>
</table>

Acknowledgments

I am indebted to Hendrik Lenstra for many useful discussions during the preparation of this paper, and to the Institute of Advanced Study for its hospitality during the same period. Bibliographical help was kindly provided by Carl Pomerance and Georges Gras, and Bert Ruitenburg performed the computations for several large primes in Table 3.3. I thank Jürgen Hurrelbrink for bringing the conjecture on “Sophie Germain primes” to my attention, and Pieter Moree for pointing out that this terminology is actually inappropriate.

Bibliography


Faculteit Wiskunde en Informatica, Universiteit van Amsterdam, Plantage Muidergracht 24, 1018 TV Amsterdam, Netherlands

E-mail address: psh@fwi.uva.nl