Numerical Verification of the Brumer-Stark Conjecture

Xavier-François Roblot, Brett Tangedal

Numerical Verification of the Brumer-Stark Conjecture

Xavier-François Roblot[1] and Brett A. Tangedal[2]

[1] CICMA, Concordia University, Montréal, Québec, CANADA
roblot@cs.concordia.ca
[2] College of Charleston, Charleston SC, 29424, USA tangedal@math.cofc.edu

1 Introduction

The construction of group ring elements that annihilate the ideal class groups of totally complex abelian extensions of $\mathbb{Q}$ is classical and goes back to work of Kummer and Stickelberger. A generalization to totally complex abelian extensions of totally real number fields was formulated by Brumer. Brumer's formulation fits into a more general framework known as the Brumer-Stark conjecture. We will verify this conjecture for a large number of examples belonging to an extended class of situations where the general status of the conjecture is still unknown. We assume throughout that k is a totally real basefield and K is a totally complex extension field, abelian over k. Let w_K denote the number of roots of unity in K, $m = [k : \mathbb{Q}]$, and $G = \mathrm{Gal}(K/k)$. We also let $S = S(K/k) = \{\mathfrak{p}_\infty^{(1)}, \ldots, \mathfrak{p}_\infty^{(m)}, \mathfrak{p}_1, \ldots, \mathfrak{p}_t\}$, where $\mathfrak{p}_\infty^{(i)}$ denotes the archimedean prime corresponding to the ith embedding of k into $\mathbb{R}$, and $\mathfrak{p}_1, \ldots, \mathfrak{p}_t$ are precisely the prime ideals in k that ramify in K. For each $\sigma \in G$, we define a corresponding partial zeta-function

$$\zeta_S(s, \sigma) = \sum_{\sigma_{\mathfrak{a}} = \sigma} \frac{1}{\mathrm{N}\mathfrak{a}^s} \tag{1}$$

where the sum is over all integral ideals $\mathfrak{a}$ of k relatively prime to the ramified primes $\mathfrak{p}_1, \ldots, \mathfrak{p}_t$ and having the same Artin symbol $(K/k, \mathfrak{a}) = \sigma_{\mathfrak{a}} = \sigma$. The infinite sum on the right side of (1) converges only for $\Re(s) > 1$, but $\zeta_S(s, \sigma)$ has a meromorphic continuation to all of $\mathbb{C}$ with exactly one (simple) pole at $s = 1$. In particular, $\zeta_S(s, \sigma)$ is analytic at $s = 0$, and based upon work of Klingen [K] and Siegel [S], we know that $\zeta_S(0, \sigma) \in \mathbb{Q}$. A more refined result, due independently to Deligne and Ribet [DR], Barsky [B], and Cassou-Noguès [CN], states that $w_K \zeta_S(0, \sigma) \in \mathbb{Z}$ for every $\sigma \in G$. Based upon this, the group ring element

$$\gamma = \gamma_{K/k} = w_K \sum_{\sigma \in G} \zeta_S(0, \sigma) \sigma^{-1}$$

lies in $\mathbb{Z}[G]$. Following Hayes [H1], we refer to γ as the Brumer element of the extension K/k. The "anti-units" of K, denoted by K°, are the elements $\alpha \in K^\times$ having absolute value one at all archimedean primes of K. Let $\mathfrak{B}$ be an arbitrary fractional ideal in K. We may now state the

BRUMER-STARK CONJECTURE: *There exists an anti-unit* $\alpha \in K^\circ$ *such that* $(\alpha) = \mathfrak{B}^\gamma$ *and* $K(\alpha^{1/w_K})$ *is abelian over* k.

Brumer originally conjectured that γ annihilates the ideal class group of K (i.e. that $\mathfrak{B}^\gamma$ is always principal). The additional feature that an anti-unit generator of the principal ideal $\mathfrak{B}^\gamma$ can be found whose w_Kth root generates an abelian extension over k is due to Stark.

Before describing our computations, we first give a brief summary of the present state of the conjecture. The Brumer-Stark conjecture has already been proved in the following cases.

(i) If $k = \mathbb{Q}$, using Stickelberger's Theorem (see [T2], p. 109).
(ii) If $[K : k] = 2$ [T1].
(iii) If $G \cong \mathbb{Z}_2 \times \mathbb{Z}_2$ in general, and when G is of exponent 2 and has order $2^l > 4$, assuming K/k is a tame extension [Sa1].
(iv) If the class number of K is one, since the conjecture is always true for principal ideals [T1].
(v) If $|G| = 4$ and K/k is a sub-extension of a non-abelian Galois extension K/k_0 of degree 8 [T1].
(vi) If K/k is a sub-extension of an abelian Galois extension K/k_0, and the Brumer-Stark conjecture is already known to be true for K/k_0 ([Sa2],[H2]).

Wiles made very important progress towards proving Brumer's part of the conjecture in [W]. For each prime p, he formulated a sub-conjecture for the $p-$part of the ideal class group of K, and showed that Brumer's conjecture follows if the sub-conjecture can be proven for every prime p. Following Wiles, Greither [G] has identified a large class of "nice" extensions and has proved that in these extensions the Brumer element annihilates the $p-$part of the ideal class group of K for all odd primes p. Working under these same restrictions, Popescu [P] has used Greither's results to deduce Stark's part of the conjecture as well. The prime 2 presents special difficulties because all of these results rely upon the Main Conjecture of Iwasawa Theory in a crucial way. Based upon this summary, we can describe the first general class of situations still unproven. The smallest basefield k would be real quadratic by (i). Since 2 always divides the relative degree $[K : k]$, the smallest unproven case would be where $G \cong \mathbb{Z}_4$ by (ii) and (iii). Therefore $[K : \mathbb{Q}] = 8$, and we restrict ourselves to those fields K whose class number exceeds one (by (iv)) and where K is non-Galois over $\mathbb{Q}$ (by (v) and (i) and (vi) combined). The suggestion that this particular class of situations be studied numerically was already made by Tate in 1981 ([T1], p. 15), but a serious computational study has only become feasible in recent years with the availability of packages such as PARI/GP [BBBCO] and KANT [DFKPRSW].

We present our computations according to the following plan. In section 2, we describe a simple method that produces an abundant supply of totally complex $\mathbb{Z}_4$ extensions over any totally real basefield. Section 3 contains our algorithm for computing the Brumer element γ, which is uniformly applicable over any totally real basefield. Section 4 gives a description of the computations required to verify the Brumer-Stark conjecture. Finally, a detailed example is presented in section 5, and section 6 contains tables and comments summarizing our computations.

2 Generating $\mathbb{Z}_4$ extensions

The following theorem appears in a paper of Nagell [N]. Let k be an arbitrary basefield. Nagell proves (Thm. 3, p. 351) that any cyclic $\mathbb{Z}_4$ extension over k can be generated by a root β of the form $\sqrt{b(1+c^2+\sqrt{1+c^2})}$ where $b, c \in k$. For our purposes, we assume k is a totally real number field and we can ensure that $K = k(\beta)$ is totally complex by choosing $b = -1$. The quartic polynomial that $\sqrt{-(1+c^2+\sqrt{1+c^2})}$ satisfies is

$$f(x) = x^4 + 2(1+c^2)x^2 + c^2(1+c^2). \tag{2}$$

Let $c \in \mathcal{O}_k$, and assume that $1+c^2 \notin k^2$. Then $f(x)$ will be irreducible over $k[x]$ by Theorem 2 of [KW] and any root of $f(x)$ will generate a totally complex $\mathbb{Z}_4$ extension K over k (see Thm. 3(ii) of [KW]).

3 Computation of the Brumer element

With a relative extension K/k defined by an irreducible polynomial $f(x)$ as in section 2, one can use the tools of a computer package (we used PARI/GP) to compute the number of roots of unity w_K, and the relative discriminant $\mathfrak{d}(K/k)$. The primes $\mathfrak{p}_1, \ldots, \mathfrak{p}_t$ dividing $\mathfrak{d}(K/k)$ are exactly the finite primes appearing in the set S. The only real task remaining in the computation of the Brumer element is the calculation of $\zeta_S(0, \sigma)$. Given $\sigma \in G$, we need a nice characterization of all integral ideals $\mathfrak{a}$ relatively prime to $\mathfrak{d}(K/k)$ which have Artin symbol $\sigma_{\mathfrak{a}} = \sigma$. A beautiful characterization is provided by the Artin Reciprocity Law [Ha] which is most elegantly formulated in terms of the conductor $\mathfrak{f}(K/k)$ of the extension K/k. The conductor of a totally complex abelian extension of a totally real number field has the form

$$\mathfrak{f}(K/k) = \mathfrak{f}\,\mathfrak{p}_\infty^{(1)} \cdots \mathfrak{p}_\infty^{(m)},$$

where $\mathfrak{f}$ is an integral ideal in k which has the exact same prime divisors as $\mathfrak{d}(K/k)$. With respect to the modulus $\mathfrak{f}(K/k)$, we obtain a partition of all fractional ideals in k relatively prime to $\mathfrak{f}$ into a finite number of classes. These classes form an abelian group, called the ray class group mod $\mathfrak{f}(K/k)$, and denoted by $G(\mathfrak{f}(K/k))$. In general, several classes will correspond to a single automorphism $\sigma \in G$ via the Artin map, and $\zeta_S(s, \sigma)$ is formed by summing over exactly the integral ideals in these classes. Even with this problem solved, we still need to analytically continue $\zeta_S(s, \sigma)$ in order to compute it at $s = 0$. The best known method to date is to decompose $\zeta_S(s, \sigma)$ into a finite sum of "sector zeta-functions" and find an analytic continuation of these latter functions. Shintani [Sh] accomplished this over any totally real basefield and found an explicit evaluation of the sector zeta-functions at $s = 0$ in terms of Bernoulli polynomials. The resulting formulas, as they stand, are impractical from an algorithmic point of view. On the other hand, one can use Shintani's evaluations in conjunction

with a geometric method involving "convexity polygons" to obtain an efficient algorithm over a real quadratic basefield [H1]. This method can be generalized to any totally real basefield k of degree m over $\mathbb{Q}$ by taking the convex closure of a set of lattice points in $\mathbb{R}^m$. Because of the resulting geometric complications, this method already has serious problems from an algorithmic standpoint when $m = 3$ (see [Kh], p. 276).

We use an alternate method which relies upon the decomposition of $\zeta_S(s, \sigma)$ into a sum of L-functions. The analytic continuation of the latter type of function is classical and dates back to Hecke. Recently, a very efficient method to compute L-function values has been used to test a related conjecture of Stark ([DST],[Ro]). We use this method here, which is based upon a formula due independently to Lavrik [L] and Friedman [F]. The relevant L-functions are defined from characters $\chi : G(\mathfrak{f}(K/k)) \to \mathbb{C}^\times$ on the ray class group mod $\mathfrak{f}(K/k)$. A given character will have a conductor of the form $\mathfrak{f}(\chi) = \mathfrak{f}_\chi \mathfrak{f}_{\chi,\infty}$, where $\mathfrak{f}_\chi$ is an integral ideal dividing $\mathfrak{f}$, and $\mathfrak{f}_{\chi,\infty}$ is a formal product of archimedean primes taken from the set $\{\mathfrak{p}_\infty^{(1)}, \ldots, \mathfrak{p}_\infty^{(m)}\}$. We always work with the *primitive* version of χ (still denoted by χ), which is defined on the ray class group mod $\mathfrak{f}(\chi)$. The corresponding L-function is defined by

$$L(s, \chi) = \prod \left(1 - \frac{\chi(\mathfrak{p})}{\mathrm{N}\mathfrak{p}^s}\right)^{-1} \quad \text{for } \Re(s) > 1,$$

with the product taken over all prime ideals in k relatively prime to $\mathfrak{f}_\chi$. If we multiply $L(s, \chi)$ by the Euler factors corresponding to primes that divide $\mathfrak{f}$ but not $\mathfrak{f}_\chi$ (there are potentially no such primes), we obtain a related function denoted by $L_S(s, \chi)$. Class field theory gives a correspondence (discussed in greater detail below) between a particular subset X_K of characters on $G(\mathfrak{f}(K/k))$ and the abelian extension K/k. In fact, the characters in X_K form a group that is isomorphic to $\mathrm{Gal}(K/k)$. The decomposition of $\zeta_S(s, \sigma)$ into a sum of L-functions mentioned above is

$$\zeta_S(s, \sigma) = \frac{1}{[K : k]} \sum_{\chi \in \mathrm{X}_K} \overline{\chi}(\mathfrak{a}) L_S(s, \chi), \tag{3}$$

where $\mathfrak{a}$ is any ideal relatively prime to $\mathfrak{f}$ such that $\sigma_\mathfrak{a} = \sigma$. All of the L-functions defined above have meromorphic continuations to the whole complex plane and all are analytic in particular at $s = 0$. Let $r(\chi)$ denote the order of the zero of the function $L(s, \chi)$ at $s = 0$.

Proposition 1. *Assume $[k : \mathbb{Q}] = m \geq 2$. For a given character χ defined on $G(\mathfrak{f}(K/k))$, we have $r(\chi) = 0$ if and only if $\mathfrak{f}_{\chi,\infty} = \mathfrak{p}_\infty^{(1)} \cdots \mathfrak{p}_\infty^{(m)}$.*

Proof. We refer to [DT] for the basic facts used here. For the trivial character, $\mathfrak{f}_{\chi_0,\infty} = 1$ and $r(\chi_0) = m - 1$ which is greater than 0 by assumption. If χ is non-trivial, then $r(\chi) = m - q$, where q is the number of archimedean primes in the formal product $\mathfrak{f}_{\chi,\infty}$.

If $L(0,\chi) = 0$ for a given χ, then clearly $L_S(0,\chi) = 0$ as well. We will have $L(0,\chi) = 0$ for at least half of the characters in X_K and so the following restriction is important. Let $\mathrm{X}_{K,\infty}$ denote the subset of characters $\chi \in \mathrm{X}_K$ such that $\mathfrak{f}_{\chi,\infty} = \mathfrak{p}_\infty^{(1)} \cdots \mathfrak{p}_\infty^{(m)}$. Then equation (3) specializes to

$$\zeta_S(0,\sigma) = \frac{1}{[K:k]} \sum_{\chi \in \mathrm{X}_{K,\infty}} \overline{\chi}(\mathfrak{a}) L_S(0,\chi). \tag{4}$$

In the following discussion, we focus on a fixed character $\chi \in \mathrm{X}_{K,\infty}$. Before we can give the Lavrik-Friedman formula for the non-zero complex number $L(0,\chi)$, we need a few preliminary definitions. Let $A_\chi = \sqrt{d_k \mathrm{N}\mathfrak{f}_\chi / \pi^m}$, where d_k is the discriminant of the field k and $\mathrm{N}\mathfrak{f}_\chi$ is the norm of the integral ideal $\mathfrak{f}_\chi$. Let $a_n(\chi)$ denote the finite sum $\sum \chi(\mathfrak{a})$ taken over all integral ideals $\mathfrak{a}$ of norm n that are relatively prime to $\mathfrak{f}_\chi$. Finally, let

$$f(x,s) = \frac{1}{2\pi i} \int_{\delta - i\infty}^{\delta + i\infty} x^z \left(\Gamma\left(\frac{z+1}{2} \right) \right)^m \frac{dz}{z-s}$$

for any $\delta > 1$. Then (see equations (4) and (5) of [DT])

$$L(0,\chi) = \frac{1}{\sqrt{\pi^m}} \sum_{n \geq 1} \left[a_n(\chi)\, f\left(\frac{A_\chi}{n}, 0 \right) + W(\chi)\, \overline{a_n(\chi)}\; f\left(\frac{A_\chi}{n}, 1 \right) \right], \tag{5}$$

where $W(\chi)$ is a complex number of absolute value one known as the "Artin root number" of χ. Let Y_χ denote the set of primes dividing $\mathfrak{f}$ but not $\mathfrak{f}_\chi$. If there exists a prime $\mathfrak{p} \in Y_\chi$ such that $\chi(\mathfrak{p}) = 1$, then $L_S(0,\chi) = 0$. Otherwise

$$L_S(0,\chi) = L(0,\chi) \prod_{\mathfrak{p} \in Y_\chi} (1 - \chi(\mathfrak{p})) \neq 0.$$

We would like to point out that Louboutin [Lo] has arrived at an equivalent form of equation (5) independently and has used it to compute relative class numbers of CM-fields. He actually gives a formula for $L(1,\chi)$, but the two values are related by $L(0,\chi) = \pi^{-m/2} W(\chi) A_\chi L(1,\overline{\chi})$ via the functional equation. Using equation (5), we can approximate $L(0,\chi)$ to any desired degree of accuracy by taking enough terms. We refer to [Lo] for detailed error bounds. The root number $W(\chi)$ is a finite sum with $\phi(\mathfrak{f}_\chi)$ terms. We refer to [DT] and [Lo] for its computation.

The method we have described thus far to compute $\zeta_S(0,\sigma)$ is applicable to any totally complex abelian extension K over a totally real field k. Throughout the remainder of this section we will assume that $G \cong \mathbb{Z}_4$. Since $G \cong \mathbb{Z}_4$, there is a ray class group character χ of order 4 corresponding to K/k, whose conductor $\mathfrak{f}(\chi)$ is equal to $\mathfrak{f}(K/k)$. The conductor of the trivial character χ_0 is of course 1. The conductors of the two characters $\chi_1 = \chi$ and $\chi_3 = \chi^3$ are equal since they are conjugate to each other. The conductor of the character $\chi_2 = \chi^2$ contains no archimedean primes and is equal to the relative discriminant of

the relative quadratic extension $k' = k(\sqrt{1+c^2})/k$. The conductor-discriminant formula [Ha] gives us the relation $\mathfrak{d}(K/k) = \mathfrak{d}(k'/k)\mathfrak{f}^2$ and thus an immediate determination of $\mathfrak{f}$. We can now compute $G(\mathfrak{f}(K/k))$, but we still have to identify the exact set of characters $\mathrm{X}_K = \{\chi_0, \chi_1, \chi_2, \chi_3\}$ corresponding to the extension K/k. To do this, we need to generate a subgroup of index 4 using relative norms. Based upon the following result of Bach and Sorenson [BS] (which assumes the ERH), we don't have to work too hard. Let

$$C = (4\log|d_K| + 2.5[K:\mathbb{Q}] + 5)^2$$

and let T denote the set of prime ideals in k of degree 1 over $\mathbb{Q}$ not dividing $\mathfrak{f}$ and having norm $\leq C$. Let H be the subgroup in $G(\mathfrak{f}(K/k))$ generated by the ideals $\mathfrak{p}^{f_\mathfrak{p}}$, where $\mathfrak{p}$ runs through T and $f_\mathfrak{p}$ denotes the residue degree of $\mathfrak{p}$ in K/k. Then $[G(\mathfrak{f}(K/k)) : H] = 4$ and the four characters on $G(\mathfrak{f}(K/k))$ which are trivial on H make up the set X_K. We have $\overline{L(s,\chi_i)} = L_S(s,\chi_i)$ for $i = 1, 3$ and $L_S(0,\chi_i) = 0$ for $i = 0, 2$. Since $L(0,\chi_1) = \overline{L(0,\chi_3)}$, we finally obtain

$$w_K\zeta_S(0,\sigma) = \frac{w_K}{2}(\Re(\overline{\chi_1}(\mathfrak{a})L(0,\chi_1))) \tag{6}$$

from equation (4). Recalling that $w_K\zeta_S(0,\sigma) \in \mathbb{Z}$, we just need to compute $L(0,\chi_1)$ to high enough accuracy to determine the *integer* on the right side of (6).

Even though we haven't made a detailed comparison between our method and the method in [H1], we believe that our method performs equally well when $m = 2$ and certainly much better when $m > 2$.

4 The Numerical Verification of the Conjecture

We begin with

Proposition 2. *Let $\mathfrak{B}_1, \ldots, \mathfrak{B}_s$ be a system of $\mathbb{Z}[G]$-generators of the ideal class group of K. Then the Brumer-Stark conjecture is true for every fractional ideal $\mathfrak{B}$ in K if and only if it is true for each ideal $\mathfrak{B}_i$ with $1 \leq i \leq s$.*

Proof. This is a direct consequence of the properties of the subgroup of fractional ideals verifying the Brumer-Stark conjecture (see [T1], p. 7).

Thus, it is enough to verify the conjecture for a finite set of ideals $\mathfrak{B}_i$, $1 \leq i \leq s$. Furthermore, a system of $\mathbb{Z}[G]$-generators can easily be extracted from a system of ideals that generate the ideal class group over $\mathbb{Z}$.

To prove that a given fractional ideal $\mathfrak{B}$ in K verifies the Brumer-Stark conjecture we proceed as follows. We first compute the ideal $\mathfrak{B}^\gamma$ and its class in the class group. If it is not principal, then the conjecture is false. Otherwise, we compute a generator β of $\mathfrak{B}^\gamma$. In general, this generator is not an anti-unit and requires modification. If an anti-unit generator α exists, then we have $\alpha = \varepsilon\beta$ for some unit ε of K. The unit ε is determined using the process described below.

We assume that $G \cong \mathbb{Z}_4 = <\sigma>$ and $[k : \mathbb{Q}] = 2$ throughout the remainder of this section.

Let $K \hookrightarrow K^{(i)} \subset \mathbb{C}$, $i = 1, 2, 3, 4$ be four non complex conjugate embeddings. For $\alpha \in K$, let $|\alpha|_i = |\alpha^{(i)}|^2$ be the normalized absolute value. Consider the classical logarithmic embedding

$$\begin{aligned} \lambda : K^\times &\to \mathbb{R}^3 \\ \alpha &\mapsto (\log|\alpha|_1, \log|\alpha|_2, \log|\alpha|_3)\,. \end{aligned}$$

The anti-units are contained in the kernel of λ, and if α exists then

$$\lambda(\varepsilon) + \lambda(\beta) = 0.$$

Let $||\cdot||$ be the Euclidean norm on $\mathbb{R}^3$ and let b be the minimal non-zero norm $||\lambda(u)||$ where u ranges through the units of K. Then the unit ε, if it exists, is the unique unit (up to some root of unity in K) satisfying

$$||\lambda(\varepsilon) + \lambda(\beta)|| < b/2.$$

This unit can be found using computation with real numbers, however once it is found, we still need to check that α possesses the required properties. The following proposition allows us to verify that α is an anti-unit.

Proposition 3. *$\alpha \in K^\circ$ if and only if $\alpha^{1+\sigma^2} = 1$.*

Proof. The automorphism σ^2 is the unique complex conjugation of the extension K/k, thus $|\alpha|_i = |\alpha^{\sigma^2}|_i$ for all i's, so $|\alpha^{1+\sigma^2}|_i = |\alpha|_i^2$ and also $\alpha^{1+\sigma^2}$ is a positive real number. Now assume that α is an anti-unit. Then $|\alpha|_i = 1$ for all i's, and thus $\alpha^{1+\sigma^2} = 1$. On the other hand, if $\alpha^{1+\sigma^2} = 1$, then $|\alpha|_i^2 = 1$ for all i's and α is an anti-unit.

Since ε is unique up to a root of unity in K, so is α. Therefore, the condition that $K(\alpha^{1/w_K})$ generates an abelian extension over k does not depend upon the choice of α. The next proposition allows us to verify this condition. We first note that $w_K = 2$ for all of the fields suggested by Tate for study (see Introduction). To see this, let L be the field generated over $\mathbb{Q}$ by the roots of unity contained in K. If $w_K > 2$, then Lk is a totally complex sub-extension of K/k. Therefore $Lk = K$ and $K/\mathbb{Q}$ is abelian, which gives a contradiction.

Proposition 4. *$K(\sqrt{\alpha})$ is abelian over k if and only if $\alpha^{\sigma-1} \in K^2$.*

Proof. This follows directly from Prop. 1.2, p. 83 of [T2].

Note that all of the required computations are done with *exact objects* and therefore give a complete verification of the Brumer-Stark conjecture for all of the examples tested and not just a verification up to the precision of the computation!

Since the prime 2 seems to play a special role in the conjecture, we make the following definition. We call the maximum power of 2 that can be factored

out of the Brumer element γ the "2-part of γ". We have actually tested the conjecture in such a way as to see how much of the 2-part of γ is really needed. More precisely, let 2^e be the 2-part of γ. We have searched for the smallest non-negative integer i such that the conjecture is true with γ replaced by $2^{i-e}\gamma$. These results are described in the last section.

5 An example

Let $k = \mathbb{Q}(\sqrt{2})$ and let K be the field generated by the polynomial (2) with $c = 3 + 3\sqrt{2}$. The discriminant d_K is $2^{31} \cdot 17^3$ and the conductor $\mathfrak{f}(K/k)$ is $\mathfrak{p}_2^7\mathfrak{p}_{17}\mathfrak{p}_\infty^{(1)}\mathfrak{p}_\infty^{(2)}$, where $\mathfrak{p}_2 = (\sqrt{2})$ is the unique prime ideal above 2 and $\mathfrak{p}_{17} = (1+3\sqrt{2})$ is one of the two prime ideals above 17. The field K is generated over $\mathbb{Q}$ by an algebraic integer θ satisfying

$$\theta^8 + 40\theta^6 + 380\theta^4 + 1360\theta^2 + 1666 = 0.$$

The field K is not Galois over $\mathbb{Q}$ and its class group is isomorphic to $\mathbb{Z}_{20} \times \mathbb{Z}_2$. Moreover, its class group is generated over $\mathbb{Z}[G]$ by the class of the ideal

$$\mathfrak{B}_1 = 3\mathcal{O}_K + (\theta + 1)\mathcal{O}_K.$$

The Galois group G of the extension K/k is generated by the automorphism

$$\sigma : \theta \mapsto \frac{1}{567}\left(5\theta^7 + 235\theta^5 + 2978\theta^3 + 8935\theta\right).$$

We compute the Brumer element and find that

$$\gamma = 8 - 16\sigma - 8\sigma^2 + 16\sigma^3 = 2^3\left(1 - 2\sigma - \sigma^2 + 2\sigma^3\right).$$

We start by testing $\gamma/8$, but the ideal $\mathfrak{B}_1^{\gamma/8}$ is not principal. Next, we look at the ideal $\mathfrak{B}_1^{\gamma/4}$ which is principal, and using the method described in the previous section we find that it is generated by the anti-unit

$$\alpha = \frac{1}{5103}\left(110\theta^7 + 98\theta^6 + 4036\theta^5 + 3724\theta^4 + 28346\theta^3 + 29288\theta^2 + 53056\theta + 63679\right).$$

However, the algebraic number $\alpha^{\sigma-1}$ is not a square in K, so the condition in Proposition 4 is not satisfied. Finally, it is clear that all the conditions are satisfied for $\gamma/2$.

Theorem 1. *The Brumer-Stark conjecture is true for this extension, it is even true if one replaces the Brumer element γ by $\gamma/2$.*

6 Tables and Summary

We used the quartic polynomial (2) with k ranging through the real quadratic fields of discriminant ≤ 500 and c ranging through the algebraic integers in k of T_2-norm ≤ 200 with $1 + c^2 \notin k^2$. Discarding the fields K obtained in this way that have class number one, are Galois over $\mathbb{Q}$, or have discriminant $\geq 10^{18}$, and keeping only non-isomorphic fields, we end up with a list of 379 fields. The Brumer-Stark conjecture has been tested for each of these field extensions using the package PARI/GP [BBBCO].

Theorem 2. *The Brumer-Stark conjecture is true for all* 379 *field extensions listed in the tables below.*

In the following tables, we list the discriminants d of the real quadratic fields considered and the corresponding elements c. We set $\omega = (1+\sqrt{d})/2$ if $d \equiv 1 \pmod 4$ and $\omega = \sqrt{d}/2$ if $d \equiv 0 \pmod 4$. The ring of integers of the real quadratic field k of discriminant d is $\mathcal{O}_k = \mathbb{Z} + \mathbb{Z}\omega$.

d	Values of c
5	$1+\omega$, $2+\omega$, $3+\omega$, $4+\omega$, $5+\omega$, $6+\omega$, 2ω, $1+2\omega$, $2+2\omega$, $3+2\omega$, $4+2\omega$, $5+2\omega$, $6+2\omega$, $8+2\omega$, $-1+3\omega$, 3ω, $1+3\omega$, $2+3\omega$, $3+3\omega$, $4+3\omega$, $5+3\omega$, $6+3\omega$, $-1+4\omega$, 4ω, $1+4\omega$, $2+4\omega$, $3+4\omega$, $4+4\omega$, $5+4\omega$, $6+4\omega$, $-2+5\omega$, $-1+5\omega$, 5ω, $1+5\omega$, $2+5\omega$, $3+5\omega$, $4+5\omega$, $5+5\omega$, $-2+6\omega$, $-1+6\omega$, 6ω, $1+6\omega$, $2+6\omega$, $3+6\omega$, $4+6\omega$, 7ω, $1+7\omega$, $2+7\omega$, $-2+8\omega$, 8ω
8	$2+\omega$, $3+\omega$, $4+\omega$, $5+\omega$, $6+\omega$, $7+\omega$, $8+\omega$, $1+2\omega$, $2+2\omega$, $4+2\omega$, $5+2\omega$, $6+2\omega$, $7+2\omega$, $8+2\omega$, $9+2\omega$, $1+3\omega$, $2+3\omega$, $3+3\omega$, $4+3\omega$, $5+3\omega$, $6+3\omega$, $7+3\omega$, $8+3\omega$, $9+3\omega$, $1+4\omega$, $2+4\omega$, $3+4\omega$, $4+4\omega$, $5+4\omega$, $6+4\omega$, $7+4\omega$, $8+4\omega$, $1+5\omega$, $2+5\omega$, $3+5\omega$, $4+5\omega$, $5+5\omega$, $6+5\omega$, $1+6\omega$, $2+6\omega$, $3+6\omega$, $4+6\omega$, $5+6\omega$
12	$3+\omega$, $4+\omega$, $5+\omega$, $6+\omega$, $7+\omega$, $8+\omega$, $9+\omega$, $1+2\omega$, $2+2\omega$, $4+2\omega$, $5+2\omega$, $6+2\omega$, $7+2\omega$, $8+2\omega$, $1+3\omega$, $2+3\omega$, $3+3\omega$, $4+3\omega$, $5+3\omega$, $6+3\omega$, $7+3\omega$, $8+3\omega$, $1+4\omega$, $2+4\omega$, $3+4\omega$, $4+4\omega$, $5+4\omega$, $6+4\omega$, $7+4\omega$, $1+5\omega$, $2+5\omega$, $3+5\omega$, $4+5\omega$, $5+5\omega$
13	ω, $1+\omega$, $2+\omega$, $3+\omega$, $4+\omega$, $5+\omega$, $8+\omega$, 2ω, $1+2\omega$, $2+2\omega$, $3+2\omega$, $4+2\omega$, $5+2\omega$, $6+2\omega$, 3ω, $1+3\omega$, $2+3\omega$, $3+3\omega$, $4+3\omega$, $5+3\omega$, $2+4\omega$, $4+4\omega$
17	ω, $1+\omega$, $2+\omega$, $3+\omega$, $4+\omega$, $5+\omega$, 2ω, $1+2\omega$, $2+2\omega$, $3+2\omega$, $4+2\omega$, $5+2\omega$, $6+2\omega$, $8+2\omega$, $2+3\omega$, $3+3\omega$, $4+3\omega$, $5+3\omega$, $6+3\omega$, $2+4\omega$
21	ω, $1+\omega$, $2+\omega$, $3+\omega$, $4+\omega$, 2ω, $1+2\omega$, $2+2\omega$, $3+2\omega$, $4+2\omega$, $5+2\omega$, $6+2\omega$, 3ω, $5+3\omega$, $2+4\omega$
24	$1+\omega$, $2+\omega$, $3+\omega$, $4+\omega$, $5+\omega$, $6+\omega$, $9+\omega$, $1+2\omega$, $2+2\omega$, $3+2\omega$, $4+2\omega$, $5+2\omega$, $6+2\omega$, $7+2\omega$, $8+2\omega$, $5+3\omega$, $6+3\omega$
28	$1+\omega$, $3+\omega$, $4+\omega$, $5+\omega$, $6+\omega$, $8+\omega$, $1+2\omega$, $2+2\omega$, $3+2\omega$, $4+2\omega$, $5+2\omega$, $6+2\omega$, $7+2\omega$, $8+2\omega$, $2+3\omega$, $4+3\omega$, $5+3\omega$, $6+3\omega$
29	ω, $1+\omega$, $2+\omega$, $3+\omega$, $4+\omega$, $6+\omega$, 2ω, $2+2\omega$, $3+2\omega$, $4+2\omega$, $5+2\omega$, $6+2\omega$, $3+3\omega$
33	ω, $1+\omega$, $2+\omega$, $3+\omega$, $4+\omega$, $4+2\omega$, $5+2\omega$, $6+2\omega$, $7+2\omega$
37	ω, $1+\omega$, $2+\omega$, $3+\omega$, $4+\omega$, $4+2\omega$, $5+2\omega$, $6+2\omega$
40	$1+\omega$, $2+\omega$, $3+\omega$, $4+\omega$, $5+\omega$, $1+2\omega$, $2+2\omega$, $3+2\omega$, $4+2\omega$, $5+2\omega$, $6+2\omega$, $7+2\omega$, $3+3\omega$
41	ω, $1+\omega$, $2+\omega$, $3+\omega$, $4+\omega$, $7+\omega$, $2+2\omega$, $4+2\omega$, $6+2\omega$

d	Values of c	d	Values of c
44	$2+\omega$, $3+\omega$, $4+\omega$, $5+\omega$, $6+\omega$, $8+\omega$, $4+2\omega$, $5+2\omega$, $6+2\omega$, $7+2\omega$	53	$2+\omega$, $3+\omega$, $4+\omega$
56	$1+\omega$, $2+\omega$, $3+\omega$, $4+\omega$, $5+\omega$, $7+\omega$, $2+2\omega$, $4+2\omega$, $5+2\omega$, $6+2\omega$	57	$1+\omega$, $2+\omega$, $3+\omega$, $4+\omega$
60	$1+\omega$, $2+\omega$, $3+\omega$, $4+\omega$, $5+\omega$, $6+\omega$, $8+\omega$	61	$2+\omega$, $3+\omega$, $4+\omega$
65	$2+\omega$, $3+\omega$, $4+\omega$	69	ω, $2+\omega$, $3+\omega$, $4+\omega$, $2+2\omega$
73	$3+\omega$, $4+\omega$	76	$1+\omega$, $2+\omega$, $3+\omega$, $4+\omega$, $5+\omega$, $6+\omega$, $8+\omega$, $1+2\omega$
77	$4+\omega$, $7+\omega$	77	$4+\omega$, $74+\omega$
88	$3+\omega$, $4+\omega$, $5+\omega$	89	$1+\omega$, $4+\omega$
92	$2+\omega$, $3+\omega$, $4+\omega$, $5+\omega$, $6+\omega$, $8+\omega$	101	$6+\omega$
104	$4+\omega$, $5+\omega$, $6+\omega$, $8+\omega$	109	$5+\omega$
113	$3+\omega$, $4+\omega$	120	$4+\omega$, $5+\omega$
124	$2+\omega$, $4+\omega$, $5+\omega$, $6+\omega$, $8+\omega$	129	$4+\omega$, $6+\omega$
136	$4+\omega$	137	$3+\omega$
140	$4+\omega$, $6+\omega$, $8+\omega$	141	$3+\omega$, $7+\omega$
149	$4+\omega$	156	$1+\omega$, $4+\omega$, $6+\omega$
161	ω	172	$4+\omega$, $6+\omega$
184	$7+\omega$	188	$4+\omega$, $6+\omega$
201	$6+\omega$	204	$6+\omega$
236	$4+\omega$	237	$4+\omega$
284	$4+\omega$	321	$1+\omega$

We now give some insight into how much of the 2-part of the Brumer element is needed for the conjecture to be true (see the comment at the end of section 4). First note that in all of our examples the Brumer element had a non-trivial 2-part. This is not generally true (see example 1, p. 172 of [H1]), but it might be true for certain classes of situations. More precisely, we have 3 examples (0.8%) for which the 2-part is 2, 207 examples (54.6%) for which it is 2^2, 123 examples (32.4%) for which it is 2^3, 40 examples (10.6%) for which it is 2^4 and 6 examples (1.6%) for which it is 2^5. In all examples, the full 2-part is not needed for the conjecture to be true. Even more striking is that in 324 examples (85.5%) only half or less than half of the 2-part is necessary and in 96 examples (25.3%) the full 2-part can be removed. The value of 2^i (i.e. the part of the 2-part needed for the conjecture to be valid) was 1 for 96 examples (25.3%), 2 for 204 examples (53.8%), 2^2 for 67 examples (17.7%), 2^3 for 11 examples (2.9%) and 2^4 for 1 example (0.3%). The values of 2^{e-i} (i.e. the maximal part of the 2-part that can be removed) was 2 for 173 examples (45.7%), 2^2 for 190 examples (50.1%) and 2^3 for 16 examples (4.2%).

The following tables list the ideal class groups of all fields K considered. Each entry consists of two parts. The first part gives the invariant factor decomposition of an abelian group A in the form $(n_1, \ldots, n_r)$ where $n_j \geq 2$ for all j and $n_{i+1} \mid n_i$ for $1 \leq i < r$. The group A has structure $\mathbb{Z}_{n_1} \times \cdots \times \mathbb{Z}_{n_r}$. The second part gives the

number of class groups isomorphic to A. Note that the smallest class number was 2 and the largest was 10064.

Occurrence of class groups with 1 invariant factor

(2)	9	(5)	2	(10)	17	(26)	4	(34)	4	(50)	3
(52)	2	(58)	3	(74)	2	(82)	2	(106)	2	(113)	1
(122)	1	(130)	5	(136)	1	(146)	1	(148)	1	(170)	1
(178)	1	(194)	1	(202)	1	(212)	1	(226)	1	(250)	1
(274)	1	(338)	1	(340)	1	(346)	1	(388)	1	(410)	1
(466)	1	(530)	1	(562)	1	(650)	1	(692)	1	(794)	1
(1130)	1	(1604)	1	(1810)	1	(1930)	1	(2026)	1	(2722)	1
(5910)	1										

Occurrence of class groups with 2 invariant factors

$(2,2)$	4	$(4,2)$	3	$(4,4)$	3	$(6,6)$	4	$(8,4)$	1	$(10,2)$	13
$(10,5)$	1	$(10,10)$	1	$(12,6)$	1	$(12,12)$	1	$(16,8)$	1	$(20,2)$	5
$(20,4)$	3	$(20,10)$	3	$(22,22)$	1	$(24,12)$	1	$(26,2)$	3	$(26,13)$	1
$(28,14)$	1	$(30,3)$	1	$(30,30)$	1	$(34,2)$	4	$(36,18)$	1	$(40,4)$	1
$(50,2)$	3	$(50,10)$	1	$(52,2)$	2	$(52,4)$	2	$(52,13)$	1	$(58,2)$	1
$(60,6)$	1	$(68,2)$	1	$(70,7)$	1	$(70,14)$	1	$(72,9)$	1	$(74,2)$	2
$(78,3)$	2	$(82,2)$	5	$(100,2)$	4	$(100,4)$	1	$(100,10)$	1	$(102,3)$	1
$(106,2)$	1	$(116,2)$	4	$(130,2)$	4	$(130,10)$	2	$(146,2)$	1	$(148,2)$	2
$(150,3)$	1	$(156,6)$	1	$(164,2)$	3	$(170,2)$	1	$(178,2)$	4	$(200,8)$	1
$(204,2)$	1	$(212,2)$	1	$(218,2)$	3	$(226,2)$	1	$(232,2)$	1	$(244,2)$	2
$(260,2)$	2	$(296,2)$	1	$(300,6)$	1	$(338,2)$	2	$(340,2)$	5	$(346,2)$	1
$(356,2)$	1	$(370,2)$	1	$(390,2)$	1	$(390,3)$	1	$(404,2)$	2	$(410,2)$	2
$(424,2)$	1	$(452,2)$	1	$(482,2)$	1	$(488,2)$	1	$(500,2)$	1	$(530,2)$	1
$(580,2)$	1	$(580,4)$	1	$(596,2)$	1	$(628,2)$	1	$(772,2)$	1	$(820,2)$	1
$(822,2)$	1	$(984,4)$	1	$(1096,2)$	1	$(1172,2)$	2	$(1220,2)$	1	$(2180,2)$	1

Occurrence of class groups with 3 invariant factors

$(4,2,2)$	2	$(4,4,2)$	3	$(4,4,4)$	2	$(8,4,2)$	3	$(10,2,2)$	3
$(10,10,2)$	1	$(12,6,2)$	2	$(16,8,2)$	1	$(16,8,4)$	1	$(16,8,8)$	1
$(18,18,2)$	1	$(20,2,2)$	10	$(20,4,2)$	5	$(20,4,4)$	1	$(20,10,2)$	2
$(20,20,2)$	3	$(20,20,4)$	1	$(24,12,2)$	1	$(26,2,2)$	3	$(28,14,2)$	3
$(34,2,2)$	3	$(40,2,2)$	1	$(40,4,2)$	1	$(40,4,4)$	1	$(40,8,2)$	1
$(40,20,2)$	1	$(44,44,2)$	1	$(50,2,2)$	2	$(52,2,2)$	3	$(52,4,2)$	2
$(58,2,2)$	1	$(60,12,2)$	1	$(60,12,6)$	1	$(68,2,2)$	4	$(68,4,2)$	1
$(100,2,2)$	1	$(100,4,2)$	2	$(100,10,2)$	1	$(104,2,2)$	2	$(104,4,4)$	1
$(104,8,4)$	1	$(106,2,2)$	2	$(116,2,2)$	3	$(120,12,2)$	1	$(130,2,2)$	1
$(148,2,2)$	2	$(178,2,2)$	1	$(194,2,2)$	1	$(202,2,2)$	1	$(244,2,2)$	1
$(250,2,2)$	1	$(260,2,2)$	1	$(274,2,2)$	1	$(290,2,2)$	1	$(292,4,2)$	1
$(340,2,2)$	2	$(340,4,2)$	1	$(404,2,2)$	1	$(520,2,2)$	1	$(596,2,2)$	1
$(740,2,2)$	1	$(1830,2,2)$	1	$(2516,2,2)$	1				

Occurrence of class groups with 4 invariant factors

$(6,6,2,2)$	1	$(8,8,2,2)$	2	$(20,2,2,2)$	1	$(20,4,2,2)$	1
$(20,4,4,2)$	1	$(20,10,2,2)$	1	$(36,36,2,2)$	1	$(52,4,2,2)$	1
$(58,2,2,2)$	1	$(68,2,2,2)$	1	$(68,4,2,2)$	1	$(82,2,2,2)$	1
$(100,4,2,2)$	1	$(104,2,2,2)$	1	$(116,4,2,2)$	1	$(122,2,2,2)$	1
$(148,2,2,2)$	1	$(200,4,2,2)$	1				

Occurrence of class groups with 5 invariant factors

$(10,2,2,2,2)$	1	$(20,2,2,2,2)$	1	$(68,4,2,2,2)$	1

Final note and acknowledgements. After having completed the full verification of the Brumer-Stark conjecture for all 379 examples listed here, Greither verified for us that all of our extensions are "nice" in the technical sense defined in his paper [G]. This makes our study of the 2-part of the Brumer element especially interesting (see comments at the end of section 1). We would like to thank Cornelius Greither for his help and we would also like to thank Igor Schein for helping us verify some of the most difficult examples.

References

[BS] E. Bach and J. Sorenson: Explicit bounds for primes in residue classes. Math. Comp. **65** (1996) 1717–1735.

[B] D. Barsky: Fonctions zêta p-adiques d'une classe de rayon des corps de nombres totalement réels. Groupe d'étude d'analyse ultramétrique 1977–78. Errata, idem 1978–79.

[BBBCO] C. Batut, K. Belabas, D. Bernardi, H. Cohen, M. Olivier: User's Guide to PARI/GP version 2.0.17, 1999.

[CN] Pierrette Cassou-Noguès: Valeurs aux entiers négatifs des fonctions zêta et fonctions zêta p-adiques. Invent. Math. **51** (1979) 29–59.

[DFKPRSW] M. Daberkow, C. Fieker, J. Klüners, M. Pohst, K. Roegner, M. Schörnig, K. Wildanger: KANT v.4. J. Symb. Comput. **24** (1997) 267-283.

[DR] P. Deligne and K. Ribet: Values of abelian L-functions at negative integers over totally real fields. Invent. Math. **59** (1980) 227–286.

[DST] David S. Dummit, Jonathan W. Sands, and Brett A. Tangedal: Computing Stark units for totally real cubic fields. Math. Comp. **66** (1997) 1239–1267.

[DT] David S. Dummit and Brett A. Tangedal: Computing the lead term of an abelian L-function. ANTS III (Buhler, Ed.) LNCS Springer-Verlag, Berlin-Heidelberg-New York, **1423** (1998) 400–411.

[F] Eduardo Friedman: Hecke's integral formula. Séminaire de Théorie des Nombres Univ. Bordeaux I, Talence (1987–88) Exposé n° 5.

[G] Cornelius Greither: Some cases of Brumer's conjecture for abelian CM extensions of totally real fields. To appear in Math. Zeit.

[Ha] Helmut Hasse: Vorlesungen über Klassenkörpertheorie. Physica-Verlag, Würzburg, 1967.

[H1] David R. Hayes: Brumer elements over a real quadratic base field. Expo. Math. **8** (1990) 137–184.

[H2] David R. Hayes: Base change for the conjecture of Brumer-Stark. J. Reine Angew. Math. **497** (1998) 83–89.

[Kh] M. Khan: Computation of partial zeta values at $s = 0$ over a totally real cubic field. J. Number Theory **57** (1996) 242–277.

[KW] L.-C. Kappe and B. Warren: An elementary test for the Galois group of a quartic polynomial. Am. Math. Monthly **96** (1989) 133–137.

[K] H. Klingen: Über die Werte der Dedekindsche Zetafunktion. Math. Ann. **145** (1962) 265–272.

[L] A. F. Lavrik: On functional equations of Dirichlet functions. English translation in Math. USSR–Izvestija **1** (1967) 421–432.

[Lo] Stéphane Louboutin: Computation of relative class numbers of CM-fields by using Hecke L-functions. Math. Comp. **69** (2000) 371–393.

[N] T. Nagell: Sur quelques questions dans la théorie des corps biquadratiques. Arkiv för Matematik **4** (1962) 347–376.

[P] Cristian Popescu: E-mail communication received on August 12th, 1999. Paper(s) forthcoming.

[Ro] Xavier-François Roblot: Algorithmes de factorisation dans les extensions relatives et applications de la conjecture de Stark à la construction des corps de classes de rayon. Thèse, Université Bordeaux I, 1997.

[Sa1] Jonathan W. Sands: Galois groups of exponent two and the Brumer-Stark conjecture. J. Reine Angew. Math. **349** (1984) 129–135.

[Sa2] Jonathan W. Sands: Abelian fields and the Brumer-Stark conjecture. Comp. Math. **53** (1984) 337–346.

[Sh] T. Shintani: On evaluation of zeta functions of totally real algebraic number fields at non-positive integers. J. Fac. Sci. Tokyo 1A **23** (1976) 393–417.

[S] C. L. Siegel: Über die Fourierschen Koeffizienten von Modulformen. Nachr. Akad. Wiss. Göttingen **3** (1970) 15–56.

[T1] John Tate: Brumer-Stark-Stickelberger. Séminaire de Théorie des Nombres Univ. Bordeaux I, Talence (1980–81) Exposé n° 24.

[T2] John Tate: Les Conjectures de Stark sur les Fonctions L d'Artin en $s = 0$. Progress in Math. Vol. 47, Birkhäuser, Boston, 1984.

[W] Andrew Wiles: On a conjecture of Brumer. Ann. Math. **131** (1990) 555–565.