

ZEROS OF 2-ADIC L -FUNCTIONS AND CONGRUENCES FOR CLASS NUMBERS AND FUNDAMENTAL UNITS

DANIEL C. SHANKS, PATRICK J. SIME, AND LAWRENCE C. WASHINGTON

ABSTRACT. We study the imaginary quadratic fields such that the Iwasawa λ_2 -invariant equals 1, obtaining information on zeros of 2-adic L -functions and relating this to congruences for fundamental units and class numbers.

This paper explores the interplay between zeros of 2-adic L -functions and congruences for fundamental units and class numbers of quadratic fields. An underlying motivation was to study the distribution of zeros of 2-adic L -functions, the basic philosophy being that the location of the zeros causes restrictions on the 2-adic behavior of the class numbers and fundamental units of real quadratic fields. Though the predicted restrictions involved the unit and class number together, numerical computations (we used PARI) revealed definite patterns for the unit and class number separately, which we were then able to prove. Several of these congruences are classical, but some of them seem to be new.

We use the information obtained to study the distribution of the zeros, in particular their distances from 1 and 0. In a previous paper [14], one of us showed that, if $(2^p + 1)/3$ is prime infinitely often, then it is possible to have zeros of 2-adic L -functions arbitrarily close to $s = 1$. Recently, Morain [7] showed that $(2^{12391} + 1)/3$ is prime, which yields a 2-adic L -function with a zero β satisfying $|\beta - 1|_2 = 2^{-6194}$ (see the discussion following Theorem 5).

In previous papers [12], [15], one of the present authors studied zeros of 3-adic L -functions in a somewhat similar approach. However, the advantage of using 2-adic L -functions for quadratic fields $\mathbb{Q}(\sqrt{m})$ is that not only is the number of zeros bounded by λ^- , the Iwasawa invariant for the cyclotomic \mathbb{Z}_2 -extension of $\mathbb{Q}(\sqrt{-m})$, but also there is a simple formula for λ^- due to Y. Kida [6] and B. Ferrero [4]. This allows us to keep the number of zeros under control. In fact, throughout the present paper we restrict ourselves to the case $\lambda^- = 1$, so we are dealing with at most one zero.

1. 2-ADIC L -FUNCTIONS

Let χ be the non-trivial Dirichlet character associated to the real quadratic field $\mathbb{Q}(\sqrt{m})$, where m is taken to be squarefree. The 2-adic L -function $L_2(s, \chi)$ satisfies

Received by the editor October 14, 1997.

1991 *Mathematics Subject Classification*. Primary 11R11; Secondary 11S40.

Key words and phrases. Quadratic fields, p -adic L -functions.

The third author was partially supported by a grant from NSA, and also thanks the Institute for Advanced Study for its hospitality during part of the preparation of this paper.

©1999 American Mathematical Society

$$L_2(1 - n, \chi) = -(1 - \chi\omega^{-n}(2)2^{n-1}) \frac{B_{n,\chi\omega^{-n}}}{n}$$

for all $n \geq 1$, where ω is the non-trivial character mod 4 and $B_{n,\chi\omega^{-n}}$ is a generalized Bernoulli number (for more on p -adic L -functions, see [13]). The 2-adic class number formula states that

$$L_2(1, \chi) = \left(1 - \frac{\chi(2)}{2}\right) \frac{2h^+ \log_2 \epsilon}{\sqrt{d}},$$

where h^+ , ϵ , and d are the class number, fundamental unit, and discriminant of $\mathbb{Q}(\sqrt{m})$, and \log_2 is the 2-adic logarithm. Iwasawa has shown that there is a power series $g(T) = g(T, \chi) \in \mathbb{Z}_2[[T]]$ such that

$$L_2(s, \chi) = 2g((1 + 4)^s - 1).$$

The Weierstrass preparation theorem says that there is a factorization

$$g(T) = P(T)U(T)$$

where $P(T)$ is a distinguished polynomial and $U(T)$ is invertible in $\mathbb{Z}_2[[T]]$. The degree of $P(T)$ is λ^- , the Iwasawa invariant for the cyclotomic \mathbb{Z}_2 -extension of $\mathbb{Q}(\sqrt{-m})$. Note that $\mathbb{Q}(\sqrt{-m})$ corresponds to the character $\chi\omega^{-1}$.

Proposition (Kida [6], Ferrero [4]). *Let $m > 4$ be squarefree and let λ^- be the Iwasawa invariant for the cyclotomic \mathbb{Z}_2 -extension of $\mathbb{Q}(\sqrt{-m})$. Then*

$$\lambda^- = -1 + \sum_{\substack{p|m \\ p \text{ odd}}} \frac{1}{8} [p^2 - 1]_2,$$

where $[n]_2 = 2^{v_2(n)}$ is the largest power of 2 dividing n .

Corollary. (a) $\lambda^- = 0$ if and only if $m = p$ or $2p$, where $p \equiv \pm 3 \pmod{8}$ is prime.

(b) $\lambda^- = 1$ if and only if m or $m/2$ is one of the following:

1. p , with $p \equiv \pm 7 \pmod{16}$
2. pq , with $p, q \equiv \pm 3 \pmod{8}$.

Let $g(T) = b_0 + b_1T + b_2T^2 + \dots$. Recall that λ^- is the index of the first coefficient b_i that is not divisible by 2. Therefore $\lambda^- = 0$ if and only if $2 \nmid b_0$, and $\lambda^- = 1$ if and only if $2 \mid b_0$ and $2 \nmid b_1$. Note that

$$2b_0 = 2g(0) = L_2(0, \chi) = -(1 - \chi\omega^{-1}(2))B_{1,\chi\omega^{-1}},$$

so $b_0 = 0$ if and only if $\chi\omega^{-1}(2) = 1$, which happens if and only if $m \equiv 7 \pmod{8}$. In this case we say that $L_2(s, \chi)$ has a trivial zero.

Let h^- be the class number of $\mathbb{Q}(\sqrt{-m})$. It is well-known that $h^- = -B_{1,\chi\omega^{-1}}$, so

$$b_0 = \frac{1}{2}(1 - \chi\omega^{-1}(2))h^-.$$

We can also consider a power series $f(T) = g\left(\frac{5}{1+T} - 1\right) = a_0 + a_1T + \dots$. Then

$$L_2(s, \chi) = 2f((1 + 4)^{1-s} - 1)$$

and $a_0 = \frac{1}{2}L_2(1, \chi)$. Since $T \mapsto \frac{5}{1+T} - 1$ is an invertible change of variables over \mathbb{Z}_2 , we find that λ^- is the index i of the first odd coefficient a_i .

Theorem 1. *Assume $\lambda^- = 1$.*

1. $v_2(b_0) \geq 1$ and $v_2(L_2(1, \chi)) \geq 2$.
2. $L_2(s, \chi)$ has a zero $\beta \in \mathbb{Z}_2$ if and only if $v_2(b_0) \geq 2$, and if and only if $v_2(L_2(1, \chi)) \geq 3$.
3. If β exists, then $v_2(\beta - 1) \geq 1$ if and only if $v_2(b_0) = 2$, and $v_2(\beta) \geq 1$ if and only if $v_2(L_2(1, \chi)) = 3$.
4. If β exists, then $v_2(L_2(1, \chi)) = v_2(\beta - 1) + 3$ and $v_2(b_0) = v_2(\beta) + 2$.

Remark. Let ψ be the quadratic character corresponding to $\mathbb{Q}(\sqrt{2})$. It follows from the work of Childress and Gold [2] that if $\lambda^- = 1$ and $L_2(s, \chi)$ has no zero in \mathbb{Z}_2 , then the zero appears one step up (if $2 \nmid m$) the \mathbb{Z}_2 -extension of the quadratic field $\mathbb{Q}(\sqrt{m})$; namely, $L_2(s, \psi\chi) = 2g(-(1+4)^s - 1)$ has a zero. This can be seen in the proof below, since in this case $(1+4)^s + 1 = -\alpha$ has a solution $s = \beta$.

Proof. The assumption that $\lambda^- = 1$ yields (1). We have $\deg P(T) = \lambda^- = 1$, so $g(T) = (T - \alpha)U(T)$ with $\alpha \in 2\mathbb{Z}_2$. Since $U(0) \in \mathbb{Z}_2^\times$, it follows that $v_2(\alpha) = v_2(b_0)$. If $L_2(\beta, \chi) = 0$, then $(1+4)^\beta - 1 = \alpha$, so $\alpha \equiv 0 \pmod{4}$, hence $v_2(b_0) \geq 2$. Moreover, $v_2(\alpha) = 2$ if and only if β is odd. Suppose now that $v_2(b_0) \geq 2$. Then $\beta = \log_2(1 + \alpha) / \log_2(1 + 4)$ is a root of $L_2(s, \chi)$. The same argument applied to $f(T)$ completes the proofs of (2) and (3).

To prove (4), let β and α be as above. Then

$$\begin{aligned} L_2(1, \chi) &= L_2(1, \chi) - L_2(\beta, \chi) \\ &= 2g(4) - 2g(\alpha) \\ &= 2(b_1(4 - \alpha) + b_2(4^2 - \alpha^2) + \dots) \\ &= 2(4 - \alpha)(b_1 + b_2(4 + \alpha) + \dots) \\ &\equiv 2(4 - \alpha) \pmod{4(4 - \alpha)}, \end{aligned}$$

since b_1 is odd and $\alpha \equiv 0 \pmod{4}$. But $\alpha - 4 = (1+4)((1+4)^{\beta-1} - 1) \equiv 4(\beta - 1) \pmod{8(\beta - 1)}$, so the first part of (4) follows. The second part follows from the same argument applied to $f(T)$. □

The above theorem expresses quantitatively the principle that a zero close to 1 causes $L_2(1, \chi)$ to be small. This can happen only if either h^+ or $\log_2 \epsilon$ is divisible by a high power of 2. On the other hand, if h^- is divisible by a high power of 2 then $\beta \in 2\mathbb{Z}_2$, which of course says that if $L_2(0, \chi)$ is small then β is forced to be near 0. Theorem 1 has the following interesting consequence.

Corollary. *Assume $\lambda^- = 1$. If $v_2(b_0) \geq 3$ then $v_2(L_2(1, \chi)) = 3$. If $v_2(L_2(1, \chi)) \geq 4$ then $v_2(b_0) = 2$.*

In particular, this implies, in the case $\lambda^- = 1$, that when h^- is divisible by a high power of 2, or if $\chi\omega^{-1}(2) = 1$, then $v_2(h^+)$ and $v_2(\log_2 \epsilon)$ are bounded. Also, if $v_2(h^+)$ or $v_2(\log_2 \epsilon)$ is large, then $v_2(h^-)$ is bounded (as long as the Euler factor does not cause a trivial zero. In the next section, we investigate this phenomenon. Our point of view is to start with $v_2(h^-)$ and see what restrictions are imposed on $v_2(h^+)$ and $v_2(\log_2 \epsilon)$. Of course, we could similarly start with $v_2(h^+) + v_2(\log_2 \epsilon)$ and study the restrictions imposed on $v_2(h^-)$. In fact, in Theorem 4(2), Theorem 5(3), Theorem 6(2), and Theorem 7(b)(1), we have $v_2(h^-) = 3$, but only inequalities for what happens with $v_2(h^+)$ and $v_2(\log_2 \epsilon)$. This is because the cause and effect are reversed: h^+ and ϵ are causing the restriction $v_2(h^-) = 3$.

2. CONGRUENCES

The above corollary implies that if $v_2(b_0) \geq 3$ then we have 2-adic restrictions on h^+ and ϵ . In this section we investigate this phenomenon.

Throughout, p and q will always denote primes. We let

h^+ = class number of $\mathbb{Q}(\sqrt{m})$,

h_0^+ = narrow class number of $\mathbb{Q}(\sqrt{m})$,

h^- = the class number of $\mathbb{Q}(\sqrt{-m})$,

$\epsilon = a + b\sqrt{m}$ = the fundamental unit of $\mathbb{Q}(\sqrt{m})$,

$\epsilon^2 = A + B\sqrt{m}$.

Recall that $h^+ = h_0^+$ if ϵ has norm -1 , and $h^+ = h_0^+/2$ if ϵ has norm $+1$.

We will often need the fact that when ϵ has norm $+1$,

$$\sqrt{\epsilon} = \sqrt{\frac{1}{2}(a+1)} + \sqrt{\frac{1}{2}(a-1)}.$$

In particular, $\frac{1}{2}(a \pm 1)$ cannot both be of the form mr^2 or r^2 with $r \in \mathbb{Q}$, since otherwise $\sqrt{\epsilon}$ would be in $\mathbb{Q}(\sqrt{m})$.

Another fact we will use often is that if $x \equiv \pm 1 \pmod{2^{3/2}}$ then $v_2(\log_2 x) = v_2(x \mp 1)$.

We start with the case of a trivial zero, so $b_0 = 0$. Since we must have $m \equiv 7 \pmod{8}$, we have either $m = p \equiv 7 \pmod{16}$ or $m = pq$ with $p \equiv 3 \pmod{8}$ and $q \equiv 5 \pmod{8}$. The following result does not seem to be well-known; we did not find it in the literature.

Theorem 2. (a) If $m = p \equiv 7 \pmod{16}$, then

$$v_2(h^+) = 0, \quad v_2(\log_2 \epsilon) = 3, \quad v_2(h^-) = 0,$$

$$a \equiv 8 \pmod{16}, \quad b \equiv \pm 3 \pmod{8}.$$

(b) If $m = pq$ with $p \equiv 3 \pmod{8}$ and $q \equiv 5 \pmod{8}$, then

$$v_2(h^+) = 1, \quad v_2(\log_2 \epsilon) = 2, \quad A \equiv \pm 31 \pmod{64}, \quad B \equiv 8 \pmod{16}.$$

Remark. In part (b), $v_2(h^-)$ is not constant. For example, when $m = 15$, $h^- = 2$ and when $m = 39$, $h^- = 4$.

Proof. (a) The fact that h^- is odd is classical. We have $(a+1)(a-1) = pb^2$. If $\gcd(a+1, a-1) = 2$ then one of $(a \pm 1)/2$ is a square and the other is p times a square. Therefore $\sqrt{\epsilon} = \sqrt{\frac{1}{2}(a+1)} + \sqrt{\frac{1}{2}(a-1)} \in \mathbb{Q}(\sqrt{p})$, which is impossible. Therefore $\gcd=1$. If $a-1 = r^2$ and $a+1 = s^2p$ for integers r, s , then $s^2p - r^2 = 2$, which is impossible mod 8. Therefore $a+1 = r^2$ and $a-1 = s^2p$, so $r^2 - s^2p = 2$. Clearly r, s are odd. Since $r^2 \equiv 2$ modulo each prime factor of s , each such factor must be $\pm 1 \pmod{8}$, so $s \equiv \pm 1 \pmod{8}$. Therefore $a = 1 + s^2p \equiv 8 \pmod{16}$. Since $a^2 - pb^2 = 1$, we must have $b \equiv \pm 3 \pmod{8}$. Therefore $\epsilon^2 = 2a^2 - 1 + 2ab\sqrt{p} \equiv -1 + 16\sqrt{p} \pmod{32}$, so $v_2(\log_2 \epsilon^2) = 4$ and $v_2(\log_2 \epsilon) = 3$. Since $3 = v_2(L_2(1, \chi)) = v_2(h^+) + v_2(\log_2 \epsilon)$, we have $v_2(h^+) = 0$.

Part (a) can also be proved as follows using quadratic forms (in fact, this was our original proof). The principal cycle for the quadratic form $x^2 - py^2$ has even length, since the fundamental unit ϵ has positive norm. Halfway through the cycle is an ambiguous form $\alpha x^2 + \beta xy + \gamma y^2$ with $\alpha = \pm 2$. This means that ± 2 is represented by the original form: $\pm 2 = x^2 - py^2$. Congruences exclude -2 . Moreover, $(x + y\sqrt{p})^2 = 2\epsilon$, which yields $a = (x^2 + py^2)/2 = x^2 - 1$ and $a - 1 = x^2 - 2 = py^2$. The proof now proceeds as above.

Since many modern readers might be somewhat unfamiliar with quadratic forms, we now restate and justify what we just did in terms of the equivalent statements for continued fractions (and we apologize to the first author). First we need the following lemma. Surely it is well known, but since we did not find a reference we prove it.

Lemma. *Let $d > 1$ be squarefree, let $\sqrt{d} = [a_0; \overline{a_1, \dots, a_n, 2a_0}]$ be the continued fraction expansion of \sqrt{d} , let $p_m/q_m = [a_0, \dots, a_m]$ be the m th convergent, and let $p_{-1} = 1$ and $q_{-1} = 0$. Let $\epsilon = p_n + q_n\sqrt{d}$ be the fundamental unit of $\mathbb{Q}(\sqrt{d})$. Then*

$$\frac{p_{n-r} + q_{n-r}\sqrt{d}}{p_{r-1} - q_{r-1}\sqrt{d}} = (-1)^{r+1}\epsilon$$

for $0 \leq r \leq n + 1$.

Proof. The case $r = 0$ is the definition of ϵ . It suffices to prove that

$$\frac{p_{n-r} + q_{n-r}\sqrt{d}}{p_{r-1} - q_{r-1}\sqrt{d}} = -\frac{p_{n-r-1} + q_{n-r-1}\sqrt{d}}{p_r - q_r\sqrt{d}}$$

for $0 \leq r \leq n$, which is equivalent to the pair of equations

$$\begin{aligned} p_{n-r}p_r - q_{n-r}q_r d + p_{n-r-1}p_{r-1} - q_{n-r-1}q_{r-1}d &= 0, \\ q_{n-r}p_r - p_{n-r}q_r + q_{n-r-1}p_{r-1} - p_{n-r-1}q_{r-1} &= 0. \end{aligned}$$

The case $r = 0$ is equivalent to

$$\sqrt{d} = ((\sqrt{d} + a_0)p_n + p_{n-1}) / ((\sqrt{d} + a_0)q_n + q_{n-1}),$$

which is well known [9, p. 114]. Assuming that the case r for the first equation has been proved, we use $p_{n-r} = a_{n-r}p_{n-r-1} + p_{n-r-2}$, and similarly for $q_{n-r}, p_{r+1}, q_{r+1}$, to rewrite the first equation as

$$\begin{aligned} (a_{n-r}p_{n-r-1} + p_{n-r-2})p_r - (a_{n-r}q_{n-r-1} + q_{n-r-2})q_r d \\ + p_{n-r-1}(p_{r+1} - a_{r+1}p_r) - q_{n-r-1}(q_{r+1} - a_{r+1}q_r)d = 0. \end{aligned}$$

Using the fact that $a_{r+1} = a_{n-r}$ and canceling the appropriate terms yields the first equation with $r + 1$ in place of r . The second equation is treated similarly. \square

We now return to the case $p \equiv 7 \pmod{16}$. Since the fundamental unit $\epsilon = a + b\sqrt{p}$ has positive norm, the value of n in the lemma must be odd. Letting $r = (n + 1)/2$ and $x = p_{r-1}, y = q_{r-1}$, we have

$$\frac{x + y\sqrt{p}}{x - y\sqrt{p}} = \pm\epsilon.$$

Therefore the primitive ideal $(x + y\sqrt{p})$ must be a product of ramified primes. Since only the primes above 2 and p ramify, we have $\pm(x^2 - py^2) = 1, 2, p, 2p$. But 1 is not possible since $r - 1 < n$. Since $|x^2 - py^2| < p$, we must have $x^2 - py^2 = \pm 2 = 2$ (the last equality obtained because of congruences mod 8). Moreover, multiplying the

numerator and denominator of the above equation by $x + y\sqrt{p}$ yields $(x + y\sqrt{p})^2 = 2\epsilon$. This justifies the steps used in the second proof above.

(b) By Theorem 1, we have $3 = v_2(L_2(1, \chi)) = v_2(h^+) + v_2(\log_2 \epsilon)$. Since three primes divide the discriminant of $\mathbb{Q}(\sqrt{m})$, $4|h_0^+$, so $2|h^+$. Therefore $v_2(\log_2 \epsilon) \leq 2$.

If a is even, then it is easy to see that $4|a$ and hence $-pqb^2 \equiv 1 \pmod{16}$. Therefore $\epsilon^2 = a^2 + pqb^2 + 2ab\sqrt{pq} \equiv -1 + 2ab\sqrt{pq} \pmod{16}$, so $\log_2(\epsilon^2) \equiv 0 \pmod{8}$. Therefore $v_2(\log_2 \epsilon) \geq 2$, and we have equality. It follows that $v_2(a) = 2$ and also $v_2(h^+) = 1$. Moreover, $v_2(\log_2 \epsilon) = 2$ implies that $B = 2ab \equiv 8 \pmod{16}$. Note that $A \equiv -1 \pmod{16}$.

If a is odd, then we must have $4|b$, hence $a^2 \equiv 1 \pmod{16}$. Therefore $\epsilon^2 \equiv 1 + 2ab\sqrt{pq} \pmod{16}$, so $v_2(\log_2 \epsilon) \geq 2$. Therefore we have equality and $v_2(b) = 2$, $v_2(h^+) = 1$. Also, $A \equiv 1 \pmod{16}$ and $B \equiv 8 \pmod{16}$.

Since $v_2(A^2 - 1) = v_2(B^2) = 6$ and we already have $A \equiv \pm 1 \pmod{16}$, we have $A \equiv \pm 31 \pmod{64}$. □

We now systematically examine the cases where $\lambda^- = 1$ and the zero, if it exists, is non-trivial. We first treat the case where m is even, since then $\chi(2) = \chi\omega^{-1}(2) = 0$, so the Euler factors disappear in the expressions for $L_2(1, \chi)$ and $L_2(0, \chi)$. Therefore

$$v_2(L_2(1, \chi)) = v_2(h^+) + v_2(\log_2 \epsilon) - \frac{1}{2}$$

in this case.

Theorem 3. *If $m = 2p$ with $p \equiv 7 \pmod{16}$, then*

$$v_2(h^+) = 0, \quad v_2(\log_2 \epsilon) = \frac{5}{2}, \quad v_2(h^-) = 2, \quad L_2(s, \chi) \text{ has no zero in } \mathbb{Z}_2$$

$$a \equiv 15 \pmod{128}, \quad b \equiv 4 \pmod{8}.$$

Proof. $v_2(h^-) = 2$ by [5, Thm. 4 and p. 596]. Therefore $v_2(b_0) = 1$. By Theorem 1, $L_2(s, \chi)$ has no zero in \mathbb{Z}_2 and $v_2(L_2(1, \chi)) = 2$.

We have $(a + 1)(a - 1) = 2pb^2$. Since a must be odd and b must be even, $(a + 1)/2$ is a square times 1, 2, p , or $2p$. The first and last on this list would imply that $\sqrt{\epsilon} \in \mathbb{Q}(\sqrt{2p})$, so 2 and p remain. If $(a + 1)/2 = pr^2$, then $(a - 1)/2 = 2s^2$, so $pr^2 - 2s^2 = 1$, which is impossible mod 8. Therefore $(a + 1)/2 = 2r^2$ and $(a - 1)/2 = ps^2$, so $2r^2 - ps^2 = 1$. Since 2 is a square modulo each prime factor of s , we have $s \equiv \pm 1 \pmod{8}$, hence $s^2 \equiv 1 \pmod{16}$. It follows that $r \equiv 2 \pmod{4}$ and $a = 4r^2 - 1 \equiv 15 \pmod{128}$. This implies that $b \equiv 4 \pmod{8}$ and $v_2(\log_2 \epsilon) = \frac{5}{2}$. Since $2 = v_2(L_2(1, \chi)) = v_2(h^+) + v_2(\log_2 \epsilon) - \frac{1}{2}$, we have $v_2(h^+) = 0$. □

Theorem 4. *Suppose $m = 2p$ with $p \equiv 9 \pmod{16}$. Then $v_2(h^-) \geq 2$.*

1. *If $v_2(h^-) = 2$ then $\text{Norm } \epsilon = -1$ and*

$$v_2(h^+) = 2, \quad v_2(\log_2 \epsilon) = \frac{1}{2}, \quad L_2(s, \chi) \text{ has no zero in } \mathbb{Z}_2,$$

$$a \equiv \pm 1 \pmod{8}, \quad b \equiv 1 \pmod{4}.$$

2. *If $v_2(h^-) = 3$ then*

$$v_2(h^+) = 1, \quad \frac{1}{2}v_2(a - 1) = v_2(b) = v_2(\log_2 \epsilon) - \frac{1}{2} = v_2(\beta - 1) + 2 \geq 3.$$

3. If $v_2(h^-) \geq 4$, then

$$v_2(h^+) = 1, \quad v_2(\log_2 \epsilon) = \frac{5}{2}, \quad v_2(\beta) = v_2(h^-) - 3 \geq 1,$$

$$a \equiv 17 \pmod{128}, \quad b \equiv 4 \pmod{8}.$$

Proof. By [5, Thm. 1 and p. 596], $v_2(h_0^+) = 2$. The valuation of h^+ therefore depends on the sign of the norm of ϵ .

Suppose $\text{Norm}(\epsilon) = +1$. Note that $a^2 - 2pb^2 = 1$ implies that a is odd and b is even. If $(a + 1)/2 = 2r^2$ and $(a - 1)/2 = ps^2$, then $2r^2 - ps^2 = 1$, so 2 is a square mod all prime divisors of s . As in Theorem 3, we find that $s^2 \equiv 1 \pmod{16}$ and $r^2 \equiv 5 \pmod{8}$, which is impossible. Therefore $(a + 1)/2 = pr^2$ and $(a - 1)/2 = 2s^2$, and $pr^2 - 2s^2 = 1$. It follows that s is even, hence $a = 1 + 4s^2 \equiv 1 \pmod{16}$. This implies that $b \equiv 0 \pmod{4}$, so $v_2(\log_2 \epsilon) \geq \frac{5}{2}$.

As in Theorem 3, if $v_2(h^-) = 2$ then $L_2(s, \chi)$ has no zero in \mathbb{Z}_2 and $v_2(L_2(1, \chi)) = 2$, so $2 = v_2(h^+) + v_2(\log_2 \epsilon) - \frac{1}{2}$. Since $4 \mid h_0^+$, we have $v_2(h^+) \geq 1$, hence $v_2(\log_2 \epsilon) \leq \frac{3}{2}$. From the above we see that we must have $\text{Norm}(\epsilon) = -1$ (this could also be obtained from [8, Thm. 2 (i) and Thm. 5] or [5, Thm. 3 and Prop. 2]). Since a and b must be odd and $\epsilon^2 = A + B\sqrt{2p} = 2a^2 + 1 + 2ab\sqrt{2p}$, we have $A \equiv 3 \pmod{16}$ and $B \equiv 2 \pmod{4}$. Therefore $\epsilon^2 \equiv -1 + 2\sqrt{2p} \pmod{4}$, so $v_2(\log_2(\epsilon^2)) = \frac{3}{2}$ and $v_2(\log \epsilon) = \frac{1}{2}$. It follows that in this case we are forced to have $v_2(h^+) = 2$ (this also follows from $v_2(h_0^+) = 2$). Since $a^2 - 2pb^2 = -1$, we see that -1 is a square modulo b , so $b \equiv 1 \pmod{4}$. Moreover, $a^2 = 2pb^2 - 1 \equiv 1 \pmod{16}$ yields $a \equiv \pm 1 \pmod{8}$.

If $v_2(h^-) \geq 3$ then $t^2 - 2pu^2 = -2$ has an integral solution by [5, Thm. 3 and Prop. 2 (β)]. By [5, p. 600], $\text{Norm}(\epsilon) = +1$, so $v_2(h^+) = v_2(h_0^+/2) = 1$.

If $v_2(h^-) \geq 4$, then Theorem 1 implies that $v_2(\beta - 1) = 0$ and $v_2(L_2(1, \chi)) = 3$. Therefore $v_2(\log_2 \epsilon) = \frac{5}{2}$. The above implies that $b \equiv 4 \pmod{8}$. Since $a^2 = 2pb^2 + 1 \equiv 33 \pmod{256}$, and since $a \equiv 1 \pmod{16}$, we have $a \equiv 17 \pmod{128}$.

If $v_2(h^-) = 3$, then $4 \leq v_2(\beta - 1) + 3 = v_2(L_2(1, \chi)) = \frac{1}{2} + v_2(\log_2 \epsilon)$. Since $v_2(a - 1) = 2v_2(b)$, we have $v_2(\log_2 \epsilon) = v_2(b) + \frac{1}{2}$. □

Theorem 5. *Suppose $m = 2pq$ with $p \equiv \pm 3 \pmod{8}$ and $q \equiv \pm 3 \pmod{8}$.*

1. *If $p \equiv q \equiv 5 \pmod{8}$ then*

$$v_2(h^+) = 2, \quad v_2(\log_2 \epsilon) = \frac{1}{2}, \quad \text{Norm } \epsilon = -1, \quad v_2(h^-) = 2,$$

$$L_2(s, \chi) \text{ has no zero in } \mathbb{Z}_2, \quad a \equiv \pm 1 \pmod{8}, \quad b \equiv 1 \pmod{4}.$$

2. *If $p \equiv 3 \pmod{8}$ and $q \equiv 5 \pmod{8}$, then*

$$v_2(h^+) = 1, \quad v_2(\log_2 \epsilon) = \frac{3}{2}, \quad v_2(h^-) = 2, \quad L_2(s, \chi) \text{ has no zero in } \mathbb{Z}_2,$$

$$a \equiv \pm 11 \pmod{32}, \quad b \equiv 2 \pmod{4}.$$

3. *If $p \equiv q \equiv 3 \pmod{8}$ then $v_2(h^-) \geq 3$ and $v_2(h^+) = 1$. If $v_2(h^-) = 3$ then*

$$3 \leq \frac{1}{2}v_2(a - 1) = v_2(b) = v_2(\log_2 \epsilon) - \frac{1}{2} = v_2(\beta - 1) + 2.$$

If $v_2(h^-) \geq 4$, then

$$2 = \frac{1}{2}v_2(a-1) = v_2(b) = v_2(\log_2 \epsilon) - \frac{1}{2},$$

$$v_2(\beta) = v_2(h^-) - 3 \geq 1.$$

Proof. Consider first the case where $p \equiv q \equiv 5 \pmod{8}$. Suppose $a^2 - 2pqb^2 = +1$. Then a is odd and b is even. If $(a+1)/2 = 2pr^2$ and $(a-1)/2 = qs^2$, then $2pr^2 - qs^2 = 1$, which is impossible mod 8. If $(a+1)/2 = pr^2$ and $(a-1)/2 = 2qs^2$, then $pr^2 - 2qs^2 = 1$, which is again impossible mod 8. If $(a \pm 1)/2 = 2r^2$ and $(a \mp 1)/2 = pqs^2$, then $2r^2 - pqs^2 = \pm 1$, which implies that ± 2 is a quadratic residue mod p , which is not the case (of course, we could switch the roles of p and q in the above, with similar results). The remaining possibilities imply that $\sqrt{\epsilon} \in \mathbb{Q}(\sqrt{2pq})$, so ϵ must have negative norm. Therefore $a^2 - 2pqb^2 = -1$, which implies that b is odd. Consequently, $a^2 \equiv 1 \pmod{16}$, so $a \equiv \pm 1 \pmod{8}$. Since -1 is a square modulo each prime factor of b , we have $b \equiv 1 \pmod{4}$. Since $\epsilon^2 = A + B\sqrt{2pq}$ with $A \equiv 3 \pmod{16}$ and $B \equiv 2 \pmod{4}$, we obtain $v_2(\log_2 \epsilon) = v_2(\log_2(\epsilon^2)) - 1 = \frac{1}{2}$. By [10, p. 191], we have $v_2(h^-) = 2$. Therefore $L_2(s, \chi)$ has no zero $\beta \in \mathbb{Z}_2$ and $2 = v_2(L_2(1, \chi)) = v_2(h^+) + v_2(\log_2 \epsilon) - \frac{1}{2}$. Therefore $v_2(h^+) = 2$.

If $p \equiv 3 \pmod{8}$ and $q \equiv 5 \pmod{8}$, then $v_2(h^-) = 2$ by [10, p. 191]. Therefore $L_2(s, \chi)$ has no zero $\beta \in \mathbb{Z}_2$ and $2 = v_2(L_2(1, \chi)) = v_2(h^+) + v_2(\log_2 \epsilon) - \frac{1}{2}$. Since $a^2 - 2pqb^2 = 1$, we have a odd and b even. The possibilities $(a+1)/2 = qr^2$ and $= 2qr^2$ are easily eliminated by congruences mod 8. If $(a \pm 1)/2 = 2r^2$ and $(a \mp 1)/2 = pqs^2$, then $2r^2 - pqs^2 = \pm 1$ implies that ± 2 is a quadratic residue mod q , which is not the case. If $(a+1)/2 = 2pr^2$ and $(a-1)/2 = qs^2$, then r and s are odd and $b = 2rs \equiv 2 \pmod{4}$. Also, $a = -1 + 4pr^2 \equiv 11 \pmod{32}$. If $(a+1)/2 = pr^2$ and $(a-1)/2 = 2qs^2$, then again r and s are odd and $b = 2rs \equiv 2 \pmod{4}$. Also, $a = 1 + 4qs^2 \equiv -11 \pmod{32}$. Therefore $v_2(\log_2 \epsilon) = \frac{3}{2}$. It follows that $v_2(h^+) = 1$.

If $p \equiv q \equiv 3 \pmod{8}$, then $v_2(h^-) \geq 3$ by [10, p. 191]. We will show below that $v_2(h^+) = 1$.

If $v_2(h^-) \geq 4$ then $v_2(b_0) \geq 3$, so Theorem 1 implies that $3 = v_2(L_2(1, \chi)) = v_2(h^+) + v_2(\log_2 \epsilon) - \frac{1}{2} = v_2(\log_2 \epsilon) + \frac{1}{2}$. Therefore $v_2(\log_2 \epsilon) = \frac{5}{2}$.

If $v_2(h^-) = 3$ then $4 \leq v_2(\beta - 1) + 3 = v_2(L_2(1, \chi)) = v_2(\log_2 \epsilon) + \frac{1}{2}$. Therefore $v_2(\log_2 \epsilon) \geq \frac{7}{2}$.

In all cases we have a odd and b even. The possibilities $(a+1)/2 = pr^2$, $= 2r^2$, and $= 2pr^2$ are eliminated by congruences mod 8 and the fact that 2 is a quadratic nonresidue mod p (and similarly with q in place of p). Therefore $(a+1)/2 = pqr^2$ and $(a-1)/2 = 2s^2$. This implies r is odd and s is even. Therefore $a = 1 + 4s^2 \equiv 1 \pmod{16}$ and hence $b \equiv 0 \pmod{4}$. This implies that $v_2(\log_2 \epsilon) \geq \frac{5}{2}$, so we have equality when $v_2(h^-) \geq 4$. In general, since $(a+1)(a-1) = 2pqb^2$ and $a+1 \equiv 2 \pmod{16}$, we have $\frac{1}{2}v_2(a-1) = v_2(b) = v_2(\log_2 \epsilon) - \frac{1}{2} = v_2(\beta - 1) + 2$.

It remains to show that $v_2(h^+) = 1$. This follows from the work of Rédei and Reichardt [11]; for the convenience of the reader, we reproduce their argument, adapted to the present situation. In the case $v_2(h^-) \geq 4$, we note that the desired result follows from $v_2(\log_2 \epsilon) \geq \frac{5}{2}$ plus the fact that $2|h^+$, so we only need to consider the case $v_2(h^-) = 3$. However, this restriction does not seem to be useful, and we consider the general case. The maximal unramified (including at ∞) elementary 2-extension of $K = \mathbb{Q}(\sqrt{2pq})$ is $K_2 = \mathbb{Q}(\sqrt{2}, \sqrt{pq})$, so the 2-class group of K is cyclic.

Suppose $4|h^+$. Then there is a unique unramified extension K_4 of K_2 that is cyclic of degree 4 over K . Moreover, $\text{Gal}(K_4/\mathbb{Q})$ is D_4 , the dihedral group of order 8. Let $I \subseteq \text{Gal}(K_4/\mathbb{Q})$ be the inertia group for some fixed prime \mathfrak{p} of K_4 above p . Then $I \cap \text{Gal}(K_4/K) = 1$. Since p has ramification degree 2 in $\mathbb{Q}(\sqrt{pq})/\mathbb{Q}$ and in K_4/\mathbb{Q} , it is unramified in $K_4/\mathbb{Q}(\sqrt{pq})$, so $I \cap \text{Gal}(K_4/\mathbb{Q}(\sqrt{pq})) = 1$. Therefore I must be one of the two subgroups $\neq \text{Gal}(K_4/K_2)$ of order 2 contained in $\text{Gal}(K_4/\mathbb{Q}(\sqrt{2}))$. In particular, I is not normal in $\text{Gal}(K_4/\mathbb{Q})$. Since I is normal in Z , the decomposition group for \mathfrak{p} , Z cannot be $\text{Gal}(K_4/\mathbb{Q})$. It follows that Z fixes $\mathbb{Q}(\sqrt{2})$, so p splits in $\mathbb{Q}(\sqrt{2})/\mathbb{Q}$. Since $p \not\equiv \pm 1 \pmod{8}$, this is a contradiction. Therefore K_4 does not exist and $v_2(h^+) = 1$. \square

In [14], the following was proved. Suppose $q = (2^n + 1)/3$ is prime. Let $m = 6q$. Then $v_2(\beta - 1) \geq (n - 3)/2$. The last part of the above theorem shows that this is an equality, since $\epsilon = 2^{n+1} + 1 + 2^{(n+1)/2}\sqrt{6q}$. The conjecture that $(2^n + 1)/3$ is prime infinitely often is discussed in [1].

The remaining cases where $\lambda^- = 1$ are of the form $\mathbb{Q}(\sqrt{m})$ with $m \equiv 1 \pmod{8}$. Therefore $\chi\omega^{-1}(2) = 0$, so the Euler factor disappears in the expression for $L_2(0, \chi)$, but $\chi(2) = 1$, so the Euler factor $(1 - \chi(2)/2) = 1/2$ cancels the 2 in the numerator of the formula for $L_2(1, \chi)$. Therefore

$$L_2(1, \chi) = \frac{h^+ \log_2 \epsilon}{\sqrt{m}} \text{ and } v_2(L_2(1, \chi)) = v_2(h^+) + v_2(\log_2 \epsilon)$$

in this case.

Theorem 6. *Let $m = p \equiv 9 \pmod{16}$. Then h^+ is odd and $v_2(h^-) \geq 2$. Also, $a \equiv 0 \pmod{4}$, $b \equiv 5 \pmod{8}$, and $v_2(\log_2 \epsilon) = v_2(a)$.*

1. *If $v_2(h^-) = 2$ then $a \equiv 4 \pmod{8}$, $A \equiv 33 \pmod{256}$, $B \equiv 8 \pmod{16}$, $v_2(\log_2 \epsilon) = 2$, and $L_2(s, \chi)$ has no zero in \mathbb{Z}_2 .*
2. *If $v_2(h^-) = 3$ then $v_2(\beta - 1) = v_2(a) - 3 \geq 1$.*
3. *If $v_2(h^-) \geq 4$ then $v_2(a) = 3$, $A \equiv 129 \pmod{1024}$, $B \equiv 16 \pmod{32}$, and $v_2(\beta) = v_2(h^-) - 3 \geq 1$.*

Proof. The fact that h^+ is odd is standard. By [5, p. 598], $v_2(h^-) \geq 2$. Also, since $p \equiv 1 \pmod{8}$, a and b are integers. Moreover, $a^2 - pb^2 = -1$, so $a \equiv 0 \pmod{4}$. Therefore $pb^2 \equiv 1 \pmod{16}$, and $b \equiv \pm 3 \pmod{8}$. Since -1 is a square mod b , we must have $b \equiv 1 \pmod{4}$, so $b \equiv 5 \pmod{8}$. Since $\epsilon^2 = 2a^2 + 1 + 2ab\sqrt{p} \equiv 1 + 2ab\sqrt{p} \pmod{4a}$, $v_2(\log_2 \epsilon) = v_2(a)$.

Assume $v_2(h^-) = 2$. Then $v_2(L_2(1, \chi)) = 2$, by Theorem 1, so $v_2(a) = v_2(\log_2 \epsilon) = 2$. The congruences for A and B follow immediately from the fact that a is 4 times an odd number, hence $a^2 \equiv 16 \pmod{128}$.

Now assume $v_2(h^-) = 3$. Then there is a zero β , and $v_2(\beta - 1) + 3 = v_2(a) = v_2(\log_2 \epsilon) = v_2(L_2(1, \chi)) \geq 4$.

Finally, if $v_2(h^-) \geq 4$ then $v_2(L_2(1, \chi)) = 3$, by the corollary to Theorem 1. This implies that $v_2(a) = v_2(\log_2 \epsilon) = 3$, which yields the desired results. \square

Theorem 7. *Let $m = pq$ with $p \equiv q \equiv \pm 3 \pmod{8}$.*

- (a) *If $p \equiv q \equiv 3 \pmod{8}$ then $v_2(h^-) = 2$, $v_2(h^+) = 0$, $a \equiv 23 \pmod{64}$, $b \equiv 4 \pmod{8}$, $v_2(\log_2 \epsilon) = 2$, and $L_2(s, \chi)$ has no zero in \mathbb{Z}_2 .*
- (b) *If $p \equiv q \equiv 5 \pmod{8}$, then $v_2(h^-) \geq 3$.*
 1. *If $v_2(h^-) = 3$, then $v_2(h^+) \geq 1$, $2v_2(B) - 1 = v_2(A - 1) \geq 5$, and $v_2(\beta - 1) = v_2(h^+) + v_2(B) - 4 \geq 1$.*

2. If $v_2(h^-) \geq 4$ then $v_2(h^+) = 1$, $v_2(\beta) = v_2(h^-) - 3 \geq 1$, $v_2(\log_2 \epsilon) = 2$, $A \equiv 33 \pmod{256}$, and $B \equiv 8 \pmod{16}$.

Remark. In part (b)(1), $v_2(h^+)$ is not constant. For example, if $m = 65$ then $h^- = 8$ and $h^+ = 2$, and if $m = 5 \times 461$ then $h^- = 24$ and $h^+ = 16$.

Proof. (a) $a^2 - pqb^2 = 1$ implies a is odd and b is even. Therefore we may assume (by switching p and q if necessary) that $(a+1)/2 = pr^2$ and $(a-1)/2 = qs^2$. This yields $pr^2 - qs^2 = 1$, hence $r \equiv 2 \pmod{4}$ and $s \equiv 1 \pmod{2}$. Therefore $a = -1 + 2pr^2 \equiv 23 \pmod{64}$. Also, $b = 2rs \equiv 4 \pmod{8}$. Therefore $v_2(\log_2 \epsilon) = 2$. By [10, Prop. 4], $v_2(h^-) = 2$, so $L_2(s, \chi)$ has no zero in \mathbb{Z}_2 and $v_2(h^+) + v_2(\log_2 \epsilon) = v_2(L_2(1, \chi)) = 2$. Therefore $v_2(h^+) = 0$.

(b) By [10, Prop. 4], $v_2(h^-) \geq 3$. If $v_2(h^-) = 3$ then $L_2(s, \chi)$ has a zero $\beta \equiv 1 \pmod{2}$. We have $4 \leq v_2(\beta - 1) + 3 = v_2(\log_2 \epsilon) + v_2(h^+)$. If $v_2(h^-) \geq 4$ then $v_2(\log_2 \epsilon) + v_2(h^+) = v_2(L_2(1, \chi)) = 3$ and $\beta \equiv 0 \pmod{2}$.

If ϵ has negative norm, then $a^2 - pqb^2 = -1$, so $a \equiv 0 \pmod{4}$, which implies that $A \equiv 1 \pmod{32}$. Since $A^2 - pqB^2 = 1$, we obtain $B \equiv 0 \pmod{8}$, hence $v_2(\log_2 \epsilon) \geq 2$. Also, if $\text{Norm } \epsilon = -1$ then $h^+ = h_0^+$. Since $2|h_0^+$, we have $v_2(h^+) \geq 1$. In the case that $v_2(h^-) \geq 4$, we therefore obtain $v_2(\log_2 \epsilon) = 2$ and $v_2(h^+) = 1$.

If ϵ has positive norm, then $a^2 - pqb^2 = +1$, so a is odd and $b \equiv 0 \pmod{4}$. We may assume $(a+1)/2 = pr^2$ and $(a-1)/2 = qs^2$, which yields $pr^2 - qs^2 = 1$. Therefore p is a square mod q (and q is a square mod p), so $4|h_0^+$ (see [5, p. 596]). Therefore $v_2(h^+) \geq 1$. Again in the case that $v_2(h^-) \geq 4$, we obtain $v_2(\log_2 \epsilon) = 2$ and $v_2(h^+) = 1$.

When $v_2(\log_2 \epsilon) = 2$, in both cases ($N\epsilon = +1$ and $N\epsilon = -1$) we have $B \equiv 8 \pmod{16}$, so $A^2 \equiv 65 \pmod{512}$. Therefore $A \equiv \pm 33 \pmod{256}$. Since $A = 2a^2 - N\epsilon = 2pqb^2 + N\epsilon \equiv 1 \pmod{32}$ in both cases, we obtain $A \equiv 33 \pmod{256}$. \square

Finally, for completeness, we list what happens when $\lambda^- = 0$. The proofs, which we omit, are very similar to those given above. Note that in this case we have both $v_2(b_0) = 0$ and $v_2(L_2(1, \chi)) = 1$, so we expect congruences for h^- , h^+ , and ϵ .

In part (2), we consider ϵ^3 instead of ϵ , since ϵ is not necessarily in $\mathbb{Z}[\sqrt{p}]$. Note that $v_2(\log_2(\epsilon^3)) = v_2(\log_2 \epsilon)$, so there is little effect on our other calculations.

Theorem 8. *Suppose $\lambda^- = 0$.*

1. If $m = p \equiv 3 \pmod{8}$, then $v_2(h^-) = 0$, $v_2(h^+) = 0$, $v_2(\log_2 \epsilon) = 1$, $a \equiv 2 \pmod{4}$, $A \equiv 7 \pmod{64}$, $B \equiv 4 \pmod{8}$.
2. If $m = p \equiv 5 \pmod{8}$, then $v_2(h^-) = 1$, $v_2(h^+) = 0$, $v_2(\log_2 \epsilon) = 1$. If $\epsilon^3 = a' + b'\sqrt{p}$ and $\epsilon^6 = A' + B'\sqrt{p}$, then $a' \equiv 2 \pmod{4}$, $b' \equiv 1 \pmod{4}$, $A' \equiv 9 \pmod{64}$, $B' \equiv 4 \pmod{8}$.
3. If $m = 2p$ with $p \equiv 3 \pmod{8}$, then $v_2(h^-) = 1$, $v_2(h^+) = 0$, $v_2(\log_2 \epsilon) = \frac{3}{2}$, $a \equiv 5 \pmod{32}$, $b \equiv 2 \pmod{4}$.
4. If $m = 2p$ with $p \equiv 5 \pmod{8}$, then $v_2(h^-) = 1$, $v_2(h^+) = 1$, $v_2(\log_2 \epsilon) = \frac{1}{2}$, $a \equiv 1 \pmod{2}$, $b \equiv 1 \pmod{2}$.

3. NUMERICAL RESULTS

Using PARI, we calculated $v_2(h^+ \log_2 \epsilon)$ and $v_2(h^-)$, and consequently $v_2(\beta - 1)$ and $v_2(\beta)$, and obtained the following data. For example, the 311 in the first row of the first table means that there are 311 primes $p \equiv 9 \pmod{16}$ less than 10^5 such that there is a zero β with $v_2(\beta - 1) = 0$ for the 2-adic L -function of the

$\mathbb{Q}(\sqrt{2p})$ with $p \equiv 9 \pmod{16}$ (cf. Theorem 4)

$v_2(\beta - 1)$	no β	0	1	2	3	4	5	6	≥ 7
$0 < p < 10^5$	601	311	160	74	26	12	7	3	2
$10^5 < p < 2 \times 10^5$	519	252	128	82	28	15	10	3	4
$2 \times 10^5 < p < 3 \times 10^5$	489	251	139	63	28	12	7	3	1
$3 \times 10^5 < p < 4 \times 10^5$	498	243	106	56	28	11	10	6	3
$4 \times 10^5 < p < 5 \times 10^5$	477	236	123	74	37	10	10	3	4
Total	2584	1293	656	349	147	60	44	18	14

$v_2(\beta)$	0	1	2	3	4	5	6	≥ 7
$0 < p < 10^5$	284	155	79	41	24	12	0	0
$10^5 < p < 2 \times 10^5$	270	134	50	30	13	20	5	0
$2 \times 10^5 < p < 3 \times 10^5$	253	132	58	31	13	12	5	0
$3 \times 10^5 < p < 4 \times 10^5$	220	137	51	32	10	6	3	4
$4 \times 10^5 < p < 5 \times 10^5$	261	120	59	30	12	6	5	4
Total	1288	678	297	164	72	56	18	8

$\mathbb{Q}(\sqrt{6q})$ with $q \equiv 3 \pmod{8}$ (cf. Theorem 5, part (3))

$v_2(\beta - 1)$	0	1	2	3	4	5	6	≥ 7
$3 < q < 10^5$	1192	582	329	144	76	39	21	25
$10^5 < q < 2 \times 10^5$	1052	493	271	128	67	30	15	30
$2 \times 10^5 < q < 3 \times 10^5$	1005	493	223	147	62	41	23	5
$3 \times 10^5 < q < 4 \times 10^5$	978	523	250	95	70	25	22	12
$4 \times 10^5 < q < 5 \times 10^5$	976	456	249	143	57	41	14	13
Total	5203	2547	1322	657	332	176	95	85

$v_2(\beta)$	0	1	2	3	4	5	6	≥ 7
$3 < q < 10^5$	1216	575	304	158	87	47	21	0
$10^5 < q < 2 \times 10^5$	1034	521	260	144	61	24	35	7
$2 \times 10^5 < q < 3 \times 10^5$	994	497	262	118	64	37	17	10
$3 \times 10^5 < q < 4 \times 10^5$	997	492	258	119	63	30	9	7
$4 \times 10^5 < q < 5 \times 10^5$	973	474	243	126	73	27	15	18
Total	5214	2559	1327	665	348	165	97	42

corresponding quadratic field $\mathbb{Q}(\sqrt{2p})$. Note that this number also gives the total number of examples of $v_2(\beta) > 0$ (i.e., the sum of the first row of the second part of the table, omitting the first entry).

These tables indicate that, for the fields considered such that β exists, $v_2(\beta - 1) = i \geq 0$ with probability approximately $2^{-(i+1)}$. Similarly, $v_2(\beta) = i \geq 0$ with probability approximately $2^{-(i+1)}$. In the families where β does not always exist, approximately half of the fields are such that β exists.

The 2-parts of the class groups of the imaginary quadratic fields considered are either cyclic (2^j) with $j \geq 2$ (for $\mathbb{Q}(\sqrt{-2p})$ and $\mathbb{Q}(\sqrt{-p})$) or of the form $(2) \times (2^j)$ with $j \geq 2$ (for $\mathbb{Q}(\sqrt{-6q})$ and $\mathbb{Q}(\sqrt{-5p})$). This follows from [11]). The philosophy of the Cohen-Lenstra heuristics [3], extended to the present situation, would predict that the occurrence of a group as the 2-part of the class group is inversely proportional to the size of its automorphism group. For the case where the 2-part

$\mathbb{Q}(\sqrt{p})$ with $p \equiv 9 \pmod{16}$ (cf. Theorem 6)

$v_2(\beta - 1)$	no β	0	1	2	3	4	5	6	≥ 7
$0 < p < 10^5$	595	309	127	88	43	15	9	7	3
$10^5 < p < 2 \times 10^5$	522	258	128	69	35	14	9	3	3
$2 \times 10^5 < p < 3 \times 10^5$	504	241	128	52	34	19	11	3	1
$3 \times 10^5 < p < 4 \times 10^5$	463	256	122	63	27	19	6	3	2
$4 \times 10^5 < p < 5 \times 10^5$	497	239	119	64	34	12	5	2	2
Total	2581	1303	624	336	173	79	40	18	11

$v_2(\beta)$	0	1	2	3	4	5	6
$0 < p < 10^5$	292	153	93	35	22	5	1
$10^5 < p < 2 \times 10^5$	261	139	64	25	15	8	7
$2 \times 10^5 < p < 3 \times 10^5$	248	132	55	28	9	9	8
$3 \times 10^5 < p < 4 \times 10^5$	242	128	72	29	17	7	3
$4 \times 10^5 < p < 5 \times 10^5$	238	123	58	29	13	6	10
Total	1281	675	342	146	76	35	29

$\mathbb{Q}(\sqrt{5p})$ with $p \equiv 5 \pmod{8}$ (cf. Theorem 7(b))

$v_2(\beta - 1)$	0	1	2	3	4	5	6	≥ 7
$5 < p < 10^5$	1192	620	306	148	58	40	14	20
$10^5 < p < 2 \times 10^5$	1061	513	275	136	68	29	17	13
$2 \times 10^5 < p < 3 \times 10^5$	1001	510	270	91	69	36	17	18
$3 \times 10^5 < p < 4 \times 10^5$	1004	492	235	137	49	25	15	16
$4 \times 10^5 < p < 5 \times 10^5$	940	475	254	122	53	30	13	14
Total	5198	2610	1340	634	297	160	76	81

$v_2(\beta)$	0	1	2	3	4	5	6	≥ 7
$5 < p < 10^5$	1206	601	300	152	76	44	18	1
$10^5 < p < 2 \times 10^5$	1051	526	276	120	85	27	17	10
$2 \times 10^5 < p < 3 \times 10^5$	1011	487	248	136	64	29	23	14
$3 \times 10^5 < p < 4 \times 10^5$	969	458	253	153	81	32	17	10
$4 \times 10^5 < p < 5 \times 10^5$	961	463	228	124	66	35	16	8
Total	4898	2535	1305	685	372	167	91	43

of the class group is cyclic of order 2^j , the automorphism group has order 2^{j-1} . Combining this with the above, we find that this extension of the Cohen-Lenstra heuristics to these cases is equivalent to the statement that $v_2(\beta) = i \geq 0$ with probability $2^{-(i+1)}$.

The elements of the automorphism group of $(2) \times (2^j)$ with $j \geq 2$ can be represented by matrices $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$, where $a = 1$, $b \in \text{Hom}(\mathbb{Z}/2\mathbb{Z}, \mathbb{Z}/2^j\mathbb{Z})$, $c \in \text{Hom}(\mathbb{Z}/2^j\mathbb{Z}, \mathbb{Z}/2\mathbb{Z})$, and $d \in \text{Aut}(\mathbb{Z}/2^j\mathbb{Z})$. Therefore this automorphism group has order 2^{j+1} . Again we find that the extension of the Cohen-Lenstra heuristics is equivalent to $v_2(\beta) = i$ with probability $2^{-(i+1)}$.

REFERENCES

1. P. T. Bateman, J. L. Selfridge, and S. S. Wagstaff, Jr., *The new Mersenne conjecture*, Am. Math. Monthly 96 (1989), 125-128. MR **90c**:11009
2. N. Childress and R. Gold, *Zeros of p -adic L -functions*, Acta Arith. 48 (1987), 63-71. MR **88i**:11091
3. H. Cohen and H. W. Lenstra, Jr., *Heuristics on class groups of number fields*, Number Theory, Noordwijkerhout 1983, 33-62, Springer Lecture Notes in Math. 1068 (1984). MR **85j**:11144
4. B. Ferrero, *The cyclotomic \mathbb{Z}_2 -extension of imaginary quadratic fields*, Amer. J. Math. **102** (1980), 447-459. MR **81g**:12006
5. P. Kaplan, *Divisibilité par 8 du nombre des classes des corps quadratiques dont le 2-groupe des classes est cyclique, et réciprocity biquadratique*, J. Math. Soc. Japan 25 (1973), 596-608. MR **48**:2113
6. Y. Kida, *On cyclotomic \mathbb{Z}_2 -extensions of imaginary quadratic fields*, Tôhoku Math. J. (2), **31** (1979), 91-96. MR **80d**:12003
7. F. Morain, e-mail announcement, April 29, 1996.
8. P. Morton, *The quadratic number fields with cyclic 2-classgroups*, Pacific J. Math. 108 (1983), 165-175. MR **84i**:12001
9. C. D. Olds, *Continued Fractions*, Random House, New York, 1963. MR **26**:3672
10. A. Pizer, *On the 2-part of the class number of imaginary quadratic number fields*, J. Number Theory 8 (1976), 184-192. MR **53**:10759
11. L. Rédei and H. Reichardt, *Die Anzahl der durch 4 teilbaren Invarianten der Klassengruppe eines beliebigen quadratischen Zahlkörpers*, J. reine angew. Math. 170 (1934), 69-74.
12. L. Washington, *Zeros of p -adic L -functions*, Sémin. Théorie des Nombres, Paris 1980-1981, Birkhäuser (1982), 337-357. MR **84f**:12008
13. L. Washington, *Introduction to cyclotomic fields*, Springer-Verlag, New York-Berlin, 1982. MR **85g**:11001
14. L. Washington, *Siegel zeros for 2-adic L -functions*, Number theory (Halifax, NS, 1994) CMS Conf. Proc., vol. 15, Amer. Math. Soc. (1995), 393-396. MR **96k**:11145
15. L. Washington, *A family of cubic fields and zeros of 3-adic L -functions*, J. Number Theory 63(1997), 408-417. MR **98e**:11126

DEPARTMENT OF MATHEMATICS, UNIVERSITY OF MARYLAND, COLLEGE PARK, MD 20742

DEPARTMENT OF MATHEMATICS & COMP. SCI., CALDWELL COLLEGE, CALDWELL, NJ 07006
E-mail address: PSime@caldwell.edu

DEPARTMENT OF MATHEMATICS, UNIVERSITY OF MARYLAND, COLLEGE PARK, MD 20742
E-mail address: lcw@math.umd.edu