BOUNDS OF THE RANK OF THE MORDELL–WEIL GROUP OF JACOBIANS OF HYPERELLIPTIC CURVES

HARRIS B. DANIELS, ÁLVARO LOZANO-ROBLEDO, AND ERIK WALLACE

Abstract. In this article we extend work of Lehmer, Shanks, and Washington on cyclic extensions, and elliptic curves associated to the simplest cubic fields. In particular, we give families of examples of hyperelliptic curves $C : y^2 = f(x)$ defined over $\mathbb{Q}$, with $f(x)$ of degree p, where p is a Sophie Germain prime, such that the rank of the Mordell–Weil group of the jacobian $J/\mathbb{Q}$ of C is bounded by the genus of C and the 2-rank of the class group of the (cyclic) field defined by $f(x)$, and exhibit examples where this bound is sharp.

1. Introduction

Let $C/\mathbb{Q}$ be a hyperelliptic curve, given by a model $y^2 = f(x)$, with $f(x) \in \mathbb{Q}[x]$, and let $J/\mathbb{Q}$ be the jacobian variety attached to C. The Mordell–Weil theorem shows that $J(\mathbb{Q})$ is a finitely generated abelian group and, therefore,

$$J(\mathbb{Q}) \cong J(\mathbb{Q})_{\text{tors}} \oplus \mathbb{Z}^{R_{J/\mathbb{Q}}},$$

where $J(\mathbb{Q})_{\text{tors}}$ is the (finite) subgroup of torsion elements, and $R_{J/\mathbb{Q}} = \text{rank}_{\mathbb{Z}}(J(\mathbb{Q})) \geq 0$ is the rank of $J(\mathbb{Q})$. In this article we are interested in bounds of $R_{J/\mathbb{Q}}$ in terms of invariants of C or $f(x)$.

In [23], Washington showed the following bound for the rank of certain elliptic curves, building on work of Shanks on the so-called simplest cubic fields (see [20]).

Theorem 1.1 ([23, Theorem 1])**.** *Let $m \geq 0$ be an integer such that $m^2 + 3m + 9$ is square-free and not divisible by 3. Let E_m be the elliptic curve given by the Weierstrass equation*

$$E_m \colon y^2 = f_m(x) = x^3 + mx^2 - (m+3)x + 1.$$

Let L_m be the number field generated by a root of $f_m(x)$, let $\text{Cl}(L_m)$ be its class group, and let $\text{Cl}(L_m)[2]$ be the 2-torsion subgroup of $\text{Cl}(L_m)$. Then,

$$\text{rank}_{\mathbb{Z}}(E_m(\mathbb{Q})) \leq 1 + \dim_{\mathbb{F}_2}(\text{Cl}(L_m)[2]).$$

In this article, we extend Washington's result to curves of genus $g \geq 2$. In order to find other families of hyperelliptic curves of genus $g \geq 2$ where a similar bound applies, we use a method of 2-descent for jacobians described by Cassels, Poonen, Schaefer, and Stoll (see Section 2; in particular, we follow the implementation described in [22]). The examples with genus $g = 2$ come from a family of cyclic quintic fields described by Lehmer ([13]).

Theorem 1.2. *Let $t \in \mathbb{Q}$, let $N(t) = t^4 + 5t^3 + 15t^2 + 25t + 25$, let*

$$f_t(x) = x^5 + t^2x^4 - 2(t^3 + 3t^2 + 5t + 5)x^3 + (N(t) - 4t^2 - 10t - 20)x^2 + (t^3 + 4t^2 + 10t + 10)x + 1,$$

1991 *Mathematics Subject Classification.* Primary: 11G10, Secondary: 14K15.

and define a hyperelliptic curve $C : y^2 = f_t(x)$ with jacobian $J/\mathbb{Q}$. Let $L/\mathbb{Q}$ be the extension defined by adjoining a root of $f_t(x)$. Then, there exists an explicit infinite set $T \subseteq \mathbb{Q}$ such that if $t \in T$, then

$$\operatorname{rank}_{\mathbb{Z}}(J(\mathbb{Q})) \leq \rho_\infty + j_\infty + \dim_{\mathbb{F}_2}(\mathrm{Cl}(L)[2]) + 4 \cdot \mu_5(N(t))$$

where $\mu_5(N(t))$ is the number of prime divisors v of the numerator of $N(t)$ such that $\nu_v(N(t)) \equiv 0 \bmod 5$, and $\rho_\infty + j_\infty \leq 4$. Moreover, if $\rho_\infty = 0$, then

$$\operatorname{rank}_{\mathbb{Z}}(J(\mathbb{Q})) \leq 2 + \dim_{\mathbb{F}_2}(\mathrm{Cl}(L)[2]) + 4 \cdot \mu_5(N(t)).$$

The set T of valid values of t mentioned in Theorem 1.2 is composed of x-coordinates of certain multiples of the generator of the Mordell–Weil group of a fixed elliptic curve over $\mathbb{Q}$ (see the statement of Theorem 4.1 for more details). For instance, the first such values of t ordered by height are

$$t = -1,\ -\frac{49721}{123201},\ -\frac{38136430641}{29144976961},\ \text{and}\ \frac{435161468382984242445545 99}{515174739418752607059465 61}.$$

Using Magma ([2]), we have verified that $\mu_5(N(t)) = 0$, for the first 6 values of $t \in T$ ordered by height (see Remark 6.6 in Section 6.2 for further details). It is also worth pointing out that Nakano ([16, Theorem 1]) has shown that $\mathrm{Cl}(L)[2]$ is always non-trivial for our choice of t.

The constants ρ_∞ and j_∞ depend on t and are, respectively, the dimensions of the kernel of signature map $\mathrm{res}_\infty : \mathcal{O}_L^\times/(\mathcal{O}_L^\times)^2 \to \{\pm 1\}^p$, and the dimension of the intersection of the image of res_∞ with a certain subgroup J_∞ (see Section 2.2 for more details). General totally real quintic fields with a totally positive system of fundamental units are expected to be extremely rare (see the heuristics and conjectures of Dummit and Voight in [6]), and one would expect that cyclic quintics with totally positive fundamental units would similarly be extremely rare, so we expect that cyclic quintic fields with $\rho_\infty = 0$ should be abundant (see 2.3 and in particular Remark 2.24).

For higher genus $g > 2$, we construct hyperelliptic curves $y^2 = f(x)$ such that $f(x)$ defines the maximal real subfield of a cyclotomic extension of $\mathbb{Q}$, and the degree of $f(x)$ is p, a Sophie Germain prime. We obtain the following result.

Theorem 1.3. *Let $q \geq 7$ be a prime such that $p = (q-1)/2$ is also prime, and let $L = \mathbb{Q}(\zeta_q)^+$ be the maximal totally real subfield of $\mathbb{Q}(\zeta_q)$. Let $f(x)$ be the minimal polynomial of $\zeta_q + \zeta_q^{-1}$ or $-(\zeta_q + \zeta_q^{-1})$, let $C/\mathbb{Q}$ be the hyperelliptic curve $y^2 = f(x)$, of genus $g = (p-1)/2$, and let $J/\mathbb{Q}$ be its jacobian. Then, there are constants ρ_∞ and j_∞, that depend on q, such that*

$$\operatorname{rank}_{\mathbb{Z}}(J(\mathbb{Q})) \leq \dim_{\mathbb{F}_2} \mathrm{Sel}^{(2)}(\mathbb{Q}, J) \leq \rho_\infty + j_\infty + \dim_{\mathbb{F}_2}(\mathrm{Cl}^+(L)[2]),$$

where $\rho_\infty + j_\infty \leq p - 1$. Further, if one of the following conditions is satisfied,

1. *the Davis–Taussky conjecture holds (Conjecture 2.19), or*
2. *the prime 2 is inert in the extension $\mathbb{Q}(\zeta_p)^+/\mathbb{Q}$, or*
3. *$q \leq 92459$,*

then $\rho_\infty = 0$ and $j_\infty = g = (p-1)/2$, and $\dim_{\mathbb{F}_2} \mathrm{Sel}^{(2)}(\mathbb{Q}, J) \leq g + \dim_{\mathbb{F}_2}(\mathrm{Cl}(L)[2])$.

In fact, if the Davis–Taussky conjecture holds (see Remark 5.4), then the bound of Theorem 1.3 becomes $\dim_{\mathbb{F}_2} \mathrm{Sel}^{(2)}(\mathbb{Q}, J) \leq g$.

The organization of the paper is as follows. In Section 2, we review the method of 2-descent as implemented by Stoll in [22]. In Sections 2.1, 2.2, and 2.4, we specialize the 2-descent method for the situations we encounter in the rest of the paper, namely the case when $f(x)$ defines a totally real extensions, or cyclic extension of $\mathbb{Q}$, of prime degree. In Section 3, we prove Washington's theorem

using the method of 2-descent. In Section 4, we prove Theorem 1.2, and in Section 5 we provide examples of hyperelliptic curves of genus $g = (p-1)/2$ where p is a Sophie Germain prime, and prove Theorem 1.3. Finally, in Section 6, we illustrate the previous sections with examples of curves, jacobians, and how their ranks compare to the bounds.

Acknowledgements. The authors would like to thank Keith Conrad, Gürkan Dogan, Franz Lemmermeyer, Paul Pollack, and Barry Smith, for several helpful comments and suggestions. We would also like to express our gratitude to David Dummit for very useful suggestions and noticing an error in an earlier version of the paper.

2. Stoll's Implementation of 2-Descent

In this section we summarize the method of 2-descent as implemented by Stoll in [22]. The method was first described by Cassels [3], and by Schaefer [19], and Poonen-Schaefer [18] in more generality. Throughout the rest of this section we will focus on computing the dimension of the 2-Selmer group of the jacobian J of a hyperelliptic curve C, given by an affine equation of the form

$$C : y^2 = f(x),$$

where $f \in \mathbb{Z}[x]$ is square-free and $\deg(f)$ is odd (Stoll also treats the case when $\deg(f)$ is even, but we do not need it for our purposes). In this case, the curve C is of genus $g = (\deg(f)-1)/2$ with a single point at infinity in the projective closure. Before we can compute the dimension of the 2-Selmer group, we must define a few objects of interest and examine some of their properties. We will follow the notation laid out in [22].

Let $\mathrm{Sel}^{(2)}(\mathbb{Q}, J)$ be the 2-Selmer group of J over $\mathbb{Q}$, and let $Ш(\mathbb{Q}, J)[2]$ be the 2-torsion of the Tate-Shafarevich group of J (as defined, for instance, in Section 1 of [22]). Selmer and Sha fit in the following fundamental short exact sequence:

$$0 \longrightarrow J(\mathbb{Q})/2J(\mathbb{Q}) \longrightarrow \mathrm{Sel}^{(2)}(\mathbb{Q}, J) \longrightarrow Ш(\mathbb{Q}, J)[2] \longrightarrow 0.$$

With this sequence in hand we get a relationship between for the rank of $J(\mathbb{Q})$ and the $\mathbb{F}_2$-dimensions of the other groups that we defined.

$$\operatorname{rank}_{\mathbb{Z}} J(\mathbb{Q}) + \dim_{\mathbb{F}_2} J(\mathbb{Q})[2] + \dim_{\mathbb{F}_2} Ш(\mathbb{Q}, J)[2] = \dim_{\mathbb{F}_2} \mathrm{Sel}^{(2)}(\mathbb{Q}, J). \tag{1}$$

Using equation (1), we get our first upper bound on the rank

$$\operatorname{rank}_{\mathbb{Z}} J(\mathbb{Q}) \leq \dim_{\mathbb{F}_2} \mathrm{Sel}^{(2)}(\mathbb{Q}, J) - \dim_{\mathbb{F}_2} Ш(\mathbb{Q}, J)[2]. \tag{2}$$

This upper bound is *computable*, in the sense that $J(\mathbb{Q})[2]$ and the Selmer group are computable, as we describe below.

Definition 2.1. *For any field extension K of $\mathbb{Q}$, let $L_K = K[T]/(f(T))$ denote the algebra defined by f and let N_K denote the norm map from L_K down to K.*

We denote $L_K = K[\theta]$, where θ is the image of T under the reduction map $K[T] \to K[T]/(f(T))$, and L_K is a product of finite extensions of K:

$$L_K = L_{K,1} \times \cdots \times L_{K,m_K},$$

where m_K is the number of irreducible factors of $f(x)$ in $K[x]$. Here, the fields $L_{K,j}$ correspond to the irreducible factors of $f(x)$ in $K[x]$, and the map $N_K : L_K \to K$ is just the product of the norms

on each component of L_K. That is, if $\alpha = (\alpha_1, \alpha_2, \ldots, \alpha_{m_K})$, then $N_K(\alpha) = \prod_{i=1}^{m_K} N_{L_{K,i}/K}(\alpha_i)$ where $N_{L_{K,i}/K} : L_{K,i} \to K$ is the usual norm map for the extension of fields $L_{K,i}/K$.

In order to ease notation, we establish the following notational conventions: when $K = \mathbb{Q}$ we will drop the field from the subscripts altogether, and if $K = \mathbb{Q}_v$, we will just use the subscript v. This convention will apply to *anything* that has a field as a subscript throughout the rest of the paper. As an example, $L_v = \mathbb{Q}_v[T]/(f(T))$ and $L = \mathbb{Q}[T]/(f(T))$.

Following standard notational conventions, we let $\mathcal{O}_K$, $I(K)$, and $\mathrm{Cl}(K)$ denote the ring of integers of K, the group of fractional ideals in K, and the ideal class group of K, respectively. We define analogous objects for the algebra L_K as products of each component, as follows:

$$\begin{aligned} \mathcal{O}_{L_K} &= \mathcal{O}_{L_{K,1}} \times \cdots \times \mathcal{O}_{L_{K,m_K}}, \\ I(L_K) &= I(L_{K,1}) \times \cdots \times I(L_{K,m_K}), \\ \mathrm{Cl}(L_K) &= \mathrm{Cl}(L_{K,1}) \times \cdots \times \mathrm{Cl}(L_{K,m_K}). \end{aligned}$$

Definition 2.2. *Let K be a field extension of $\mathbb{Q}$, and let $L = \mathbb{Q}[T]/(f(T))$ be as before.*

(1) Let $I_v(L)$ denote the subgroup of $I(L)$ consisting of prime ideals in L with support above a prime v in $\mathbb{Z}$. For a finite set S of places of $\mathbb{Q}$, let

$$I_S(L) = \prod_{v \in S \setminus \{\infty\}} I_v(L).$$

(2) For any field extension K of $\mathbb{Q}$, let

$$H_K = \ker\left(N_K \colon L_K^\times/(L_K^\times)^2 \to K^\times/(K^\times)^2\right).$$

For any place v of $\mathbb{Q}$, we let $\mathrm{res}_v \colon H \to H_v$ be the canonical restriction map induced by the natural inclusion of fields $\mathbb{Q} \hookrightarrow \mathbb{Q}_v$.

(3) Let $\mathrm{Div}^0_-(C)$ denote the group of degree-zero divisors on C with support disjoint from the principal divisor $\mathrm{div}(y)$.

Remark 2.3. In our case, the curve is given by $C : y^2 = f(x)$, and the support of $\mathrm{div}(y)$ is exactly the points with coordinates $(\alpha, 0)$, where α is a root of f, and the unique point at infinity.

Now for each K, there is a homomorphism

$$F_K \colon \mathrm{div}(C)(K) \to L_K^\times, \quad \sum_P n_P P \mapsto \prod_P (x(P) - \theta)^{n_P},$$

and this homomorphism induces a homomorphism $\delta_K \colon J(K) \to H_K$ with kernel $2J(K)$ by [22, Lemma 4.1]. By abusing notation, we also use δ_K to denote the induced map $J(K)/2J(K) \to H_K$.

All of these facts, together with some category theory, give us the following characterization of the 2-Selmer group of J over $\mathbb{Q}$.

Proposition 2.4 ([22, Prop. 4.2])**.** *The 2-Selmer group of J over $\mathbb{Q}$ can be identified as follows:*

$$\mathrm{Sel}^{(2)}(\mathbb{Q}, J) = \{\xi \in H \mid \mathrm{res}_v(\xi) \in \delta_v(J(\mathbb{Q}_v)) \text{ for all } v\}.$$

In order to take advantage of this description of the Selmer group, we need some additional facts about the 2-torsion of J and the δ_K maps.

Lemma 2.5 ([22, Lemma 4.3])**.** *Let K be a field extension of $\mathbb{Q}$.*

(1) *For a point $P \in C(K)$ not in the support of $\mathrm{div}(y)$, $\delta_K(P - \infty) = x(P) - \theta \bmod (L_K^\times)^2$.*

(2) *Let $f = f_1 \cdots f_{m_K}$ be the factorization of f over K into monic irreducible factors. Then, to every factor f_j, we can associate an element $P_j \in J(K)[2]$ such that:*
   (i) *The points $\{P_j\}$ generate $J(K)[2]$ and satisfy $\sum_{j=1}^{m_K} P_j = 0$.*
   (ii) *Let h_j be the polynomial such that $f = f_j h_j$. Then*

$$\delta_K(P_j) = (-1)^{\deg(f_j)} f_j(\theta) + (-1)^{\deg(h_j)} h_j(\theta) \bmod (L_K^\times)^2.$$

(3) $\dim J(K)[2] = m_K - 1$.

Definition 2.6. *Let $I_v = \ker(N\colon I_v(L)/I_v(L)^2 \to I(\mathbb{Q})/I(\mathbb{Q})^2)$ and let $\mathrm{val}_v\colon H_v \to I_v$ be the map induced by the valuations on each component of L_v. Considering all primes at once, we get another map $\mathrm{val}\colon H \to I(L)/I(L)^2$. More specifically, the* val *map is the product of $\mathrm{val}_v(\mathrm{res}_v)$ over all places v.*

Next, the following lemma helps us compute the dimensions of various groups when K is a local field or $\mathbb{R}$.

Lemma 2.7 ([22, Lemma 4.4])**.** *Let K be a v-adic local field, and let $d_K = [K : \mathbb{Q}_2]$ if $v = 2$ and $d_K = 0$ if v is odd. Then*

(1) $\dim J(K)/2J(K) = \dim J(K)[2] + d_K g = m_K - 1 + d_K g$.
(2) $\dim H_K = 2 \dim J(K)/2J(K) = 2(m_K - 1 + d_K g)$.
(3) $\dim I_K = m_K - 1$.

With all of this machinery the description of $\mathrm{Sel}^{(2)}(\mathbb{Q}, J)$ given in Proposition 2.4 can be refined as follows.

Proposition 2.8 ([22, Cor. 4.7])**.** *Let $S = \{\infty, 2\} \cup \{v : v^2$ divides $\mathrm{disc}(f)\}$. Then*

$$\mathrm{Sel}^{(2)}(\mathbb{Q}, J) = \{\xi \in H \mid \mathrm{val}(\xi) \in I_S(L)/I_S(L)^2,\ \mathrm{res}_v(\xi) \in \delta_v(J(\mathbb{Q}_v)) \text{ for all } v \in S\}.$$

This new characterization suggests the following method to compute $\mathrm{Sel}^{(2)}(\mathbb{Q}, J)$:

S1: Find the set S.
S2: For each $v \in S$, determine $J_v = \delta_v(J(\mathbb{Q}_v)) \subseteq H_v$.
S3: Find a basis for a suitable finite subgroup $\widetilde{H} \subseteq L^\times/(L^\times)^2$ such that $\mathrm{Sel}^{(2)}(\mathbb{Q}, J) \subseteq \widetilde{H}$.
S4: Compute $\mathrm{Sel}^{(2)}(\mathbb{Q}, J)$ as the inverse image of $\prod_{v\in S} J_v$ under

$$\prod_{v\in S} \mathrm{res}_v\colon \widetilde{H} \to \prod_{v\in S} H_v.$$

Ignoring any complications that arise from computing and factoring the discriminant of f, we focus on steps 2 and 3. We omit the details of how to carry out step 4, since we are only interested in an upper bound for the $\mathbb{F}_2$-dimension of $\mathrm{Sel}^{(2)}(J, \mathbb{Q})$. Step 2 can be broken down into three substeps:

S2.1: For all $v \in S \setminus \{\infty\}$, compute $J_v = \delta_v(J(\mathbb{Q}_v))$ and its image $G_v = \mathrm{val}_v(J_v)$ in I_v.
S2.2: If $G_v = 0$ for some v, with v odd, remove v from S.
S2.3: Compute J_∞.

To complete step 2.3, we need the following lemma.

Lemma 2.9 ([22, Lemma 4.8])**.** *With notation as above:*

(1) $\dim J(\mathbb{R})/2J(\mathbb{R}) = m_\infty - 1 - g$.
(2) *J_∞ is generated by the $\delta_\infty(P_\infty)$ for $P \in C(\mathbb{R})$.*

(3) *The value of $\delta_\infty(P-\infty)$ only depends on the connected component of $C(\mathbb{R})$ containing P.*

Next, for step 3, we see that if we let

$$G = \prod_{v\in S\setminus\{\infty\}} G_v \subseteq I(L)/I(L)^2,$$

then the group $\{\xi \in H : \mathrm{val}(\xi) \in G\}$ contains $\mathrm{Sel}^{(2)}(\mathbb{Q}, J)$. In fact, the larger group $\widetilde{H} = \{\xi \in L^\times/(L^\times)^2 : \mathrm{val}(\xi) \in G\}$ also contains the 2-Selmer group and we can compute its basis using the following two steps.

S3.1: Find a basis of $V = \ker(\mathrm{val}\colon L^\times/(L^\times)^2 \to I(L)/I(L)^2)$.

S3.2: Enlarge this basis to get a basis of $\widetilde{H} = \mathrm{val}^{-1}(G)$.

With notation as above, Stoll deduces an upper bound and a formula for the $\mathbb{F}_2$-dimension of the 2-Selmer group (see Lemma 4.10 and the discussion under Step 4), as follows.

Proposition 2.10 ([22, Lemma 4.10])**.** *With notation as above,*

$$\dim_{\mathbb{F}_2} \mathrm{Sel}^{(2)}(\mathbb{Q}, J) \leq (m_\infty - 1) + \dim_{\mathbb{F}_2}(\mathrm{Cl}(L)[2]) + \dim_{\mathbb{F}_2} \ker\big(G \to \mathrm{Cl}(L)/2\mathrm{Cl}(L)\big).$$

In the next section, we modify the proof of the bound in Proposition 2.10 to allow for extra conditions at infinity, before we specialize to totally real, and cyclic extensions.

2.1. **About the proof of Proposition 2.10.** The following commutative diagrams helps understand where the Selmer group fits:

$$\begin{array}{ccccccc}
0 & \longrightarrow & J(\mathbb{Q})/2J(\mathbb{Q}) & \xrightarrow{\delta} & H & \xrightarrow{\mathrm{val}} & I(L)/I(L)^2 \\
 & & \downarrow & & \downarrow{\scriptstyle \prod_v \mathrm{res}_v} & & \downarrow \\
0 & \longrightarrow & \prod_v J(\mathbb{Q}_v)/2J(\mathbb{Q}_v) & \xrightarrow{\prod_v \delta_v} & \prod_v H_v & \xrightarrow{\prod_v \mathrm{val}_v} & \prod_v I_v(L)/I_v(L)^2
\end{array}$$

The 2-Selmer group of J over $\mathbb{Q}$ is then given, as in Prop. 2.8, by

$$\mathrm{Sel}^{(2)}(\mathbb{Q}, J) = \{\xi \in H : \mathrm{val}(\xi) \in I_S(L)/I_S(L)^2,\ \mathrm{res}_v(\xi) \in \delta_v(J(\mathbb{Q}_v)) \text{ for all } v \in S\}.$$

The Selmer group is thus contained in $H \subseteq L^\times/(L^\times)^2$, and more precisely,

$$\mathrm{Sel}^{(2)}(\mathbb{Q}, J) \subseteq \{\xi \in H : \mathrm{val}(\xi) \in G,\ \mathrm{res}_\infty(\xi) \in J_\infty\}$$

where $J_\infty = \delta_\infty(J(\mathbb{R}))$, the group G is the product $\prod_{v\in S\setminus\{\infty\}} G_v \subseteq I(L)/I(L)^2$, and recall that H is the kernel of the norm map from $L^\times/(L^\times)^2$ down to $\mathbb{Q}^\times/(\mathbb{Q}^\times)^2$. Thus, $\mathrm{Sel}^{(2)}(\mathbb{Q}, J)$ is contained in the larger group

$$\widehat{H} = \{\xi \in L^\times/(L^\times)^2 : \mathrm{val}(\xi) \in G,\ \mathrm{res}_\infty(\xi) \in J_\infty\}.$$

We emphasize here that the definition of $\widetilde{H}$ in [22] does not impose a condition at ∞, but the definition of $\widehat{H}$ does to improve the bounds accuracy (thus $\widehat{H} \subseteq \widetilde{H}$). In an attempt to simplify notation, let L_{J_∞} be the subspace of $L^\times/(L^\times)^2$ with a condition added at infinite primes by $L_{J_\infty} = L^\times/(L^\times)^2 \cap \mathrm{res}_\infty^{-1}(J_\infty)$. Thus, $\widehat{H} = \{\xi \in L_{J_\infty} : \mathrm{val}(\xi) \in G\}$, and $\mathrm{Sel}^{(2)}(\mathbb{Q}, J) \subseteq \widehat{H}$. Note that $\widehat{H}$ is the largest such subgroup $\subseteq L^\times/(L^\times)^2$ with

$$\mathrm{val}(\widehat{H}) \cong G \cap \mathrm{val}\left(L_{J_\infty}\right).$$

Let us define subspaces V and W of $L^\times/(L^\times)^2$ as follows:

- Let $\{\xi_i\}$ be generators of $G \cap \mathrm{val}\,(L_{J_\infty})$, and let W be the subspace generated by $\{\mathrm{val}^{-1}(\xi_i)\}$. Note that $W \subseteq L_{J_\infty} \subseteq L^\times/(L^\times)^2$. In particular, $\mathrm{res}_\infty(w) \in J_\infty$ for all $w \in W$. Moreover, W and $\mathrm{val}(W)$ are isomorphic by construction, so
$$W \cong \mathrm{val}(W) = G \cap \mathrm{val}\,(L_{J_\infty}) \subseteq G \cap \mathrm{val}\left(L^\times/(L^\times)^2\right) = \ker(G \to \mathrm{Cl}(L)/2\mathrm{Cl}(L)).$$
Thus, $\dim(W) \leq \dim \ker(G \to \mathrm{Cl}(L)/2\mathrm{Cl}(L))$.
- Next, let us write $V = \ker(\mathrm{val}\colon L_{J_\infty} \to I(L)/I(L)^2)$. It follows that $\widehat{H} = V \oplus W$ (note that $\mathrm{val}(V)$ is trivial, while $\mathrm{val}(w)$ is non-trivial for every $w \neq 0$ in W).

Lemma 2.11. *Let $V = \ker(\mathrm{val}\colon L_{J_\infty} \to I(L)/I(L)^2)$, let $U = \left(\mathcal{O}_L^\times/(\mathcal{O}_L^\times)^2\right) \cap L_{J_\infty}$, and let $\mathrm{Cl}(L_{J_\infty})$ be the class group defined as follows $\mathrm{Cl}(L_{J_\infty}) = I(L)/P(L_{J_\infty})$, where $I(L)$ is the group of fractional ideals of L, and $P(L_{J_\infty})$ is the group of principal fractional ideals $\mathfrak{A} = (\alpha)$ with a generator such that $\mathrm{res}_\infty(\alpha) \in J_\infty$. Then, there is an exact sequence:*
$$0 \mapsto U \to V \to \mathrm{Cl}(L_{J_\infty})[2] \to 0,$$
where
$$\mathrm{Cl}(L_{J_\infty})[2] = \{[\mathfrak{A}] \in \mathrm{Cl}(L_{J_\infty})[2] : \mathfrak{A}^2 = (\alpha) \text{ for some } \alpha \in L_{J_\infty}\}.$$

Proof. Consider
$$\begin{array}{ccccccccc} & & L^\times \cap \mathrm{res}_\infty^{-1}(J_\infty) & \xrightarrow{2} & L^\times \cap \mathrm{res}_\infty^{-1}(J_\infty) & \longrightarrow & L_{J_\infty} & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & & \downarrow{\scriptstyle \mathrm{val}} & & \\ 0 & \longrightarrow & I(L) & \xrightarrow{2} & I(L) & \longrightarrow & I(L)/I(L)^2 & \longrightarrow & 0 \end{array}$$
and apply the snake lemma. □

Remark 2.12. Let $P(L)$ be the subgroup of all principal fractional ideals, let $P^+(L)$ be the subgroup of principal ideals generated by a totally positive element, and let $P(L_{J_\infty})$ be as above. Since the trivial signature $(1, 1, \ldots, 1) \in J_\infty$, it implies that $P^+(L) \subseteq P(L_{J_\infty}) \subseteq P(L)$, and therefore there are inclusions
$$\mathrm{Cl}(L) \subseteq \mathrm{Cl}(L_{J_\infty}) \subseteq \mathrm{Cl}^+(L),$$
where $\mathrm{Cl}^+(L)$ is the narrow class group of L.

Putting all this together (and writing dim for $\dim_{\mathbb{F}_2}$), we obtain a bound
$$\begin{aligned} \dim \mathrm{Sel}^{(2)}(\mathbb{Q}, J) &\leq \dim(\widehat{H}) = \dim U + \dim \mathrm{Cl}(L_{J_\infty})[2] + \dim W \\ &= \dim\left(\mathcal{O}_L^\times/(\mathcal{O}_L^\times)^2 \cap \mathrm{res}_\infty^{-1}(J_\infty)\right) + \dim \mathrm{Cl}(L_{J_\infty})[2] + \dim G \cap \mathrm{val}\,(L_{J_\infty}) \\ &\leq \dim\left(\mathcal{O}_L^\times/(\mathcal{O}_L^\times)^2 \cap \mathrm{res}_\infty^{-1}(J_\infty)\right) + \dim \mathrm{Cl}^+(L)[2] + \dim G \cap \mathrm{val}\,(L_{J_\infty})\,. \end{aligned} \tag{3}$$
We note here that $\dim\left(\mathcal{O}_L^\times/(\mathcal{O}_L^\times)^2 \cap \mathrm{res}_\infty^{-1}(J_\infty)\right) \leq m_\infty - 1$, where we have used the fact that $\dim(\mathcal{O}_L^\times/(\mathcal{O}_L^\times)^2) = m_\infty$, and the fact that $\mathrm{res}_\infty(-1)$ is not in J_∞ (because $J_\infty = \delta_\infty(J(\mathbb{R})) \subseteq H_\infty$, which is the kernel of the norm map, so $N(j) = 1$ for $j \in J_\infty$, but the norm $N(-1) = -1$ because the degree of L is odd). We will improve on the bound given by (3) above by making certain assumptions about G and a more careful analysis of the dimension of the subgroup of totally positive units. Before we state our refinements, we review some of the results on totally positive units that we shall need.

2.2. **Totally Positive Units.** Let L be a totally real Galois number field of prime degree $p > 2$, with embeddings $\tau_i : L \to \mathbb{R}$, for $i = 1, \dots, p$, and maximal order $\mathcal{O}_L$. Let $\mathrm{Cl}(L) = \mathrm{Cl}(\mathcal{O}_L)$ be the ideal class group of L, and let $\mathrm{Cl}^+(L)$ be the narrow class group. Let $V_\infty = \{\pm 1\}^p \cong (\mathbb{F}_2)^p$ and define

$$\mathrm{res}_\infty : L^\times/(L^\times)^2 \to V_\infty$$

by $\mathrm{res}_\infty(\alpha) = (\tau_1(\alpha), \tau_2(\alpha), \dots, \tau_p(\alpha))$. Let $\mathcal{O}_L^\times$ be the unit group of $\mathcal{O}_L$, and let $\mathcal{O}_L^{\times,+}$ be the subgroup of totally positive units. Thus,

$$\ker\left(\mathrm{res}_\infty|_{\mathcal{O}_L^\times/(\mathcal{O}_L^\times)^2}\right) = \mathcal{O}_L^{\times,+}/(\mathcal{O}_L^\times)^2.$$

We refer the reader to [6] for heuristics and conjectures about the dimension of the totally positive units (in particular, the conjecture on page 4). In the following theorem, we use the notation of [6].

Theorem 2.13. *Let ρ, ρ^+, and ρ_∞ be defined by*

$$\rho = \dim_{\mathbb{F}_2} \mathrm{Cl}(L)/2\mathrm{Cl}(L), \;\; \rho^+ = \dim_{\mathbb{F}_2} \mathrm{Cl}^+(L)/2\mathrm{Cl}^+(L), \;\; \textit{and } \rho_\infty = \dim_{\mathbb{F}_2} \mathcal{O}_L^{\times,+}/(\mathcal{O}_L^\times)^2$$

Then,

(1) $\rho_\infty = p - \dim_{\mathbb{F}_2} \mathrm{res}_\infty(\mathcal{O}_L^\times/(\mathcal{O}_L^\times)^2) = \dim_{\mathbb{F}_2}\{\pm 1\}^p/\mathrm{res}_\infty(\mathcal{O}_L^\times/(\mathcal{O}_L^\times)^2)$.

(2) We have

$$0 \to \{\pm 1\}^p/\mathrm{res}_\infty(\mathcal{O}_L^\times/(\mathcal{O}_L^\times)^2) \to \mathrm{Cl}^+(L) \to \mathrm{Cl}(L) \to 0.$$

In particular, $\max\{\rho, \rho_\infty\} \le \rho^+ \le \rho_\infty + \rho$, *and* $\rho^+ = \rho_\infty + \rho$ *if and only if the exact sequence splits.*

(3) (Armitage-Fröhlich) $\rho^+ - \rho \le (p-1)/2$.

Proof. For part (1), note that $\rho_\infty = \dim_{\mathbb{F}_2} \mathcal{O}_L^{\times,+}/(\mathcal{O}_L^\times)^2$ is the dimension of $\ker\left(\mathrm{res}_\infty|_{\mathcal{O}_L^\times/(\mathcal{O}_L^\times)^2}\right)$, and the dimension of $\mathcal{O}_L^\times/(\mathcal{O}_L^\times)^2$ is p. Thus, the dimension of the image of $\mathrm{res}_\infty|_{\mathcal{O}_L^\times/(\mathcal{O}_L^\times)^2}$ is p minus the dimension of the kernel.

For part (2), see Section 2 of [6], and in particular Equation (2.9). Part (3) is shown in [1], where it is shown that $\rho^+ - \rho \le \lfloor r_1/2 \rfloor$, where r_1 is the number of real embeddings of L. Here $r_1 = p$ is an odd prime, so the proof is concluded. □

From the statement of the previous theorem, we see that $\rho^+ \ge \rho_\infty$. However, $\rho \ge \rho_\infty$ is not necessarily true. In the following result, a condition is given that implies $\rho \ge \rho_\infty$ (see also [11], Section 3).

Theorem 2.14 ([17, Corollaire 2c])**.** *Let $L/\mathbb{Q}$ be a finite abelian extension with Galois group of odd exponent n, and suppose that -1 is congruent to a power of 2 modulo n. Then, in the notation of Theorem 2.13, we have $\rho = \rho^+$. In particular, $\rho \ge \rho_\infty$.*

We obtain the following corollary.

Corollary 2.15. *Let $L/\mathbb{Q}$ be a cyclic extension of odd prime degree p, and suppose that the order of 2 in $(\mathbb{Z}/p\mathbb{Z})^\times$ is even. Then, $\rho = \rho^+$. In particular,* $\dim_{\mathbb{F}_2} \mathrm{Cl}(L)[2] = \dim_{\mathbb{F}_2} \mathrm{Cl}^+(L)[2]$.

Proof. Suppose that $\mathrm{Gal}(L/\mathbb{Q}) \cong \mathbb{Z}/p\mathbb{Z}$ for some prime $p > 2$, such that the order of 2 in $(\mathbb{Z}/p\mathbb{Z})^\times$ is even (since $\mathrm{Gal}(L/\mathbb{Q})$ is cyclic of order p, this is equivalent to -1 being congruent to a power of 2 modulo p). Hence, Theorem 2.14 applies, and $\rho = \rho^+$. □

The odd primes below 100 such that the order of 2 is odd modulo p are 7, 23, 31, 47, 71, 73, 79, and 89, so the corollary applies to all other primes not in this list (i.e., 3, 5, 11, 13, 17, 19, etc.).

Theorem 2.16 ([9]). *Let $K/\mathbb{Q}$ be a real abelian extension of the rationals of degree n, let h_K be the class number of K, and let $C_K \subseteq \mathcal{O}_K^\times$ the groups of circular units of K (as defined in [9], p. 376), and let $C_K^+ \subseteq \mathcal{O}_K^{\times,+}$ be the subgroup of circular units that are totally positive. Let K^+ be the maximal real subfield of K, and let h_K^+ be its class number. Let $h_K^- = h_K/h_K^+$. Further, assume that each prime p which ramifies in K does not split. Then:*

1. *The index $[\mathcal{O}_K^{\times,+} : (\mathcal{O}_K^\times)^2]$ is a divisor of the index $[C_K^+ : C_K^2]$.*
2. *If the discriminant of K is plus or minus a power of a prime, then h_K^- is odd if and only if $[C_L^+ : C_L^2] = 1$, where C_L is the subgroup of circular units of $L = K^+$.*
3. *Suppose the discriminant of K is plus or minus a power of a prime, $[K^+ : \mathbb{Q}] = n$ is a power of an odd prime p, and the order of $2 \bmod p$ is even. Then, h_K^- is odd if and only if h_K^+ is odd.*

Proof. The results are, respectively, Lemma 5, Theorem 3, and Theorem 4 of [9]. □

Next, we cite a results of Estes which extends work of Davis ([5, Corollary 2]), and Stevenhagen ([21, Theorem 2.5]). See also [12, Theorems 3.1 and 3.3].

Theorem 2.17 ([8]). *Let q and p be primes such that $q = 2p + 1$. If 2 is inert in $\mathbb{Q}(\zeta_p)^+$, where ζ_p is a primitive p-th root of unity, then the class number of $\mathbb{Q}(\zeta_q)$ is odd.*

The following result combines the results of Davis, Estes, Stevenhagen, and Garbanati, and gives a specific criterion to check that $\rho_\infty = 0$ for the maximal real subfield of a cyclotomic field.

Theorem 2.18. *Let q and $p > 2$ be primes such that $q = 2p+1$, and let $L = \mathbb{Q}(\zeta_q + \zeta_q^{-1})$, where ζ_q is a primitive q-th root of unity. Further, assume that the prime 2 is inert in the extension $\mathbb{Q}(\zeta_p)^+/\mathbb{Q}$. Then, $\rho_\infty = \dim_{\mathbb{F}_2} \mathcal{O}_L^{\times,+}/(\mathcal{O}_L^\times)^2 = 0$.*

Proof. Let $K = \mathbb{Q}(\zeta_q)$ and let $K^+ = L = \mathbb{Q}(\zeta_q + \zeta_q^{-1})$. We note that the discriminant of K is a power of a prime (namely q), and therefore the primes of K or L that are ramified (namely the primes above q), are totally ramified, so they do not split. Moreover, $p = (q-1)/2$ is prime and $[L : \mathbb{Q}] = p$. Thus, the hypotheses of Theorem 2.16 are satisfied for K and L.

If 2 is inert in $\mathbb{Q}(\zeta_p)^+/\mathbb{Q}$, then Theorem 2.17 shows that h_K is odd, and therefore h_K^- is odd as well, since $h_K^- = h_K/h_K^+$ by definition. Since the discriminant of K is a power of q, Theorem 2.16 part (2) shows that $[C_L^+ : C_L^2] = 1$ and therefore $[\mathcal{O}_L^{\times,+} : (\mathcal{O}_L^\times)^2] = 1$ as well by part (1). We conclude that $\rho_\infty = 0$. □

There is in fact a conjecture of Davis and Taussky that says that $\rho_\infty = 0$ in the case of $L = \mathbb{Q}(\zeta_q + \zeta_q^{-1})$, where $p = (q-1)/2$ is a Sophie Germain prime. For more on the Davis–Taussky conjecture see [5], [7], [8], [12], and [21].

Conjecture 2.19 (Davis–Taussky conjecture). *Let q and p be primes such that $q = 2p + 1$, and let $L = \mathbb{Q}(\zeta_q + \zeta_q^{-1})$, where ζ_q is a primitive q-th root of unity. Then, $C_L^+ = C_L^2$. (Thus, it follows that $\rho_\infty = \dim_{\mathbb{F}_2} \mathcal{O}_L^{\times,+}/(\mathcal{O}_L^\times)^2 = 0$.)*

In the next result we note that the Davis–Taussky conjecture is equivalent to the class number of $\mathbb{Q}(\zeta_q)$ being odd. (We thank David Dummit for pointing out the following equivalence to us.)

Theorem 2.20. *Let q and p be primes such that $q = 2p + 1$, let $L = \mathbb{Q}(\zeta_q + \zeta_q^{-1})$, where ζ_q is a primitive q-th root of unity, and let $K = \mathbb{Q}(\zeta_q)$. Then, $C_L^+ = C_L^2$ if and only if the class number of K is odd.*

Proof. If h_K^+ is even, then h_K^- is even (see, for instance, [21], pp. 773-774, for a proof of this fact). Since $h_K = h_K^+ h_K^-$, it follows that h_K^- is odd if and only if h_K is odd. Since the discriminant of K is a power of q (prime), Theorem 2.16, part (2), implies that h_K^- is odd if and only if $C_L^+ = (C_L)^2$. Hence, the Davis–Taussky conjecture holds if and only if h_K^- is odd, if and only if h_K is odd. □

We conclude this section with some remarks about how to compute an upper bound of ρ_∞ in the cyclic case, working in coordinates over $\mathbb{F}_2$. Let L be a cyclic extension of $\mathbb{Q}$ of degree $p > 2$, and let $\mathrm{Gal}(L/\mathbb{Q}) = \langle\sigma\rangle$. Then, L is totally real (since L is Galois over $\mathbb{Q}$, then it is totally real or totally imaginary, so $[L : \mathbb{Q}] = p > 2$ is odd, and $p = 2r_2$ is impossible). Let $u \neq \pm 1$ be a fixed (known) unit in $\mathcal{O}_L^\times$ and let

$$\mathrm{res}_\infty(u) = (\varepsilon_1, \ldots, \varepsilon_p)$$

where $\tau_1, \ldots, \tau_p$ are the real embeddings of L and ε_i is the sign of $\tau_i(u) \in \mathbb{R}$. We order our embeddings in the following manner. Let $g_u(x)$ be the minimal polynomial of u over $\mathbb{Q}$, and let $r_1, \ldots, r_p$ be the real roots of $g_u(x)$ ordered so that $r_1 < r_2 < \cdots < r_p$. Then, $\{r_i\} = \{\tau_j(u)\}$, and we choose τ_i so that $\tau_i(u) = r_i$ for all $1 \leq i \leq p$. With this notation, $\mathrm{res}_\infty(u) = (-1, -1, -1, \ldots, 1, 1, 1)$, i.e., it consists of a non-negative number of -1 signs followed by a non-negative number of $+1$ signs. Recall that u is in the kernel of res_∞ if and only if u is a totally positive unit.

Attached to the generator $\sigma \in \mathcal{G} = \mathrm{Gal}(L/\mathbb{Q})$, there is a permutation $\phi = \phi_\sigma \in S_p$, where ϕ is considered here as a permutation of $\{1, 2, \ldots, n\}$, such that $\tau_i(\sigma(u)) = r_{\phi(i)}$, and therefore

$$\mathrm{res}_\infty(\sigma(u)) = (\varepsilon_{\phi(1)}, \ldots, \varepsilon_{\phi(p)}).$$

Since τ is an embedding (injective), if $\tau_i(\alpha) = r_i$, then $\tau_i(\sigma(\alpha)) = r_{\phi(i)}$. It follows that $\tau_i(\sigma^n(u)) = r_{\phi^n(i)}$, and

$$\mathrm{res}_\infty(\sigma^n(u)) = (\varepsilon_{\phi^n(1)}, \ldots, \varepsilon_{\phi^n(p)}),$$

for all $n \geq 1$.

Now, in addition, suppose that u is a unit of norm 1, and let $\mathcal{G} \cdot u$ be the subgroup of units generated by the conjugates of u, i.e.,

$$\mathcal{G} \cdot u = \langle u, \sigma(u), \sigma^2(u), \ldots, \sigma^{p-1}(u)\rangle \subseteq \mathcal{O}_L^\times$$

generate a subgroup of $\mathcal{O}_L^\times$. Note that the product $\prod_{n=0}^{p-1} \sigma^n(u) = 1$, so

$$\mathcal{G} \cdot u = \langle u, \sigma(u), \sigma^2(u), \ldots, \sigma^{p-2}(u)\rangle.$$

Then,

$$\mathrm{res}_\infty(\mathcal{G} \cdot u) = \langle (\varepsilon_{\phi^n(1)}, \ldots, \varepsilon_{\phi^n(p)}) : 0 \leq n \leq p-2\rangle \subseteq V_\infty,$$

where we have defined $V_\infty = \{\pm 1\}^p$. If we fix an isomorphism $\psi : \{\pm 1\} \cong \mathbb{F}_2$, and write $f_i = \psi(\varepsilon_i)$, then the map $\mathrm{res}_\infty : \mathcal{G} \cdot u \to V_\infty$ can be written in $\mathbb{F}_2$-coordinates, and the corresponding $p \times (p-1)$ matrix over $\mathbb{F}_2$ is given by

$$M_{\infty,u} = \left(f_{\phi^j(i)}\right)_{\substack{1 \leq i \leq p \\ 0 \leq j \leq p-2}} = \begin{pmatrix} f_1 & f_{\phi(1)} & \cdots & f_{\phi^{p-2}(1)} \\ f_2 & f_{\phi(2)} & \cdots & f_{\phi^{p-2}(2)} \\ \vdots & \vdots & \ddots & \vdots \\ f_p & f_{\phi(p)} & \cdots & f_{\phi^{p-2}(p)} \end{pmatrix}.$$

Lemma 2.21. *Let u be a unit of norm 1, and let $d_{\infty,u}$ be the dimension of the column space of $M_{\infty,u}$ or, equivalently, the dimension of $\mathrm{res}_\infty(\mathcal{G}\cdot u)$. Then, $\rho_\infty \le (p-1) - d_{\infty,u}$. In particular, if $d_{\infty,u} = p-1$, then $\rho_\infty = 0$.*

Proof. If u is of norm 1, then $-1 \notin \mathcal{G}\cdot u$, because the norm of -1 is -1, and the norm of every element in $\mathcal{G}\cdot u$ is 1. In particular, $\langle \mathrm{res}_\infty(-1), \mathrm{res}_\infty(\mathcal{G}\cdot u)\rangle$ is a space of dimension $1+d_{\infty,u}$. Hence, the kernel of res_∞ is at most of dimension $p-(1+d_{\infty,u})$. It follows that $\rho_\infty \le (p-1)-d_{\infty,u}$ as desired. □

2.3. **Totally positive units in cyclic extensions of prime degree.** Let L be a cyclic extension of prime degree $p>2$, and let $\mathcal{O}_L^\times$ be the unit group of $\mathcal{O}_L$. Let $\mathcal{O}_L^{\times,1}$ be the units of norm 1, so that $\mathcal{O}_L^\times \cong \{\pm 1\}\times \mathcal{O}_L^{\times,1}$. In this section we show the following result:

Proposition 2.22. *Let $p\ge 3$ be a prime, let L be a cyclic extension of degree p, and suppose that the polynomial $\phi_p(x) = (x^p-1)/(x-1)$ is irreducible over $\mathbb{F}_2$. Then, either $\rho_\infty = 0$ (i.e., $\mathcal{O}_L^{\times,+} = (\mathcal{O}_L^\times)^2$), or $\rho_\infty = p-1$ in which case every unit in $\mathcal{O}_L^{\times,1}$ is totally positive.*

Proof. If every unit in $\mathcal{O}_L^{\times,1}$ is totally positive, then $\rho_\infty = p-1$ since we would have

$$\rho_\infty = \dim_{\mathbb{F}_2} \mathcal{O}_L^{\times,+}/(\mathcal{O}_L^\times)^2 = \dim_{\mathbb{F}_2} \mathcal{O}_L^{\times,1}/(\mathcal{O}_L^\times)^2 = p-1.$$

Otherwise, there must be a unit $u\in\mathcal{O}_L^{\times,1}$ that is not totally positive (in particular, u is not in $\pm 1\cdot(\mathcal{O}_L^\times)^2$). Let $G = \mathrm{Gal}(L/\mathbb{Q}_p) = \langle\sigma\rangle \cong \mathbb{Z}/p\mathbb{Z}$, and let $u_i = \sigma^i(u)$ for $i=0,\dots,p-1$, be the conjugates of u. Let τ be a fixed embedding of L in $\mathbb{R}$, let $\tau(u_i)=\varepsilon_i\in\{\pm1\}$ for $i=0,\dots,p-1$, and order the embeddings $\tau=\tau_0,\dots,\tau_{p-1}$ of L such that $\mathrm{res}_\infty(u) = (\varepsilon_0,\dots,\varepsilon_{p-1})$. In other words, $\tau_i = \tau\circ\sigma^i$. Thus,

$$\mathrm{res}_\infty(\sigma(u)) = \mathrm{res}_\infty(u_1) = (\varepsilon_1,\dots,\varepsilon_{p-1},\varepsilon_0).$$

Consider the class $\overline{u}\in\mathcal{O}_L^\times/(\mathcal{O}_L^\times)^2$ and its non-trivial signature $\mathrm{res}_\infty(u)$. The group ring $\mathbb{F}_2[G]$ acts on the module $M = \mathbb{F}_2[G]\cdot\overline{u}$. Since G is of prime order, it follows that M is irreducible. Furthermore, since $u\neq\pm1$ it follows that $\mathrm{res}_\infty(u)\neq(1,1,\dots,1)$ or $(-1,-1,\dots,-1)$. Hence, $\mathrm{res}_\infty(\sigma(u))\neq\mathrm{res}_\infty(u)$ by our formula above, and therefore M is not 1-dimensional.

Moreover,

$$\mathbb{F}_2[G]\cong\mathbb{F}_2[x]/(x^p-1)\cong\mathbb{F}_2[x]/(x-1)\oplus\mathbb{F}_2[x]/(\phi_p(x)),$$

Since we are assuming that $\phi_p(x)$ is irreducible over $\mathbb{F}_2$, the only irreducible representations of G over $\mathbb{F}_2$ are the trivial (1-dimensional) representation, and a representation of dimension $p-1$. Since the irreducible $\mathbb{F}_2[G]$-module M is not 1-dimensional, it must be $(p-1)$-dimensional. Finally, we note that $M\subseteq\mathcal{O}_L^{\times,1}/(\mathcal{O}_L^\times)^2$, and every unit class in M has non-trivial signature (the norm is 1 and there are $p>2$ signs, so both 1 and -1 appear in the signature). Since the dimension of all possible signatures in $\mathcal{O}_L^{\times,1}$ is $p-1$, and M is $(p-1)$-dimensional, we conclude that all signatures occur, and therefore $\rho_\infty = 0$, as desired. □

We conclude this section quoting a conjectural density of cubic fields and quintic fields with maximal ρ_∞, which is part of a broader conjecture of Dummit and Voight (see [6]).

Conjecture 2.23 ([6])**.** *Let $p=3$ (resp. $p=5$). As L varies over all totally real fields of degree p ordered by absolute discriminant, the density of such fields with $\rho_\infty = 2$ (resp. $\rho_\infty = 4$) is approximately* 1.9% *(resp.* 0.000019%*).*

Remark 2.24. By Prop. 2.22, if L is a cyclic field of degree $p = 5$, and $\rho_\infty \neq 4$, then it must be 0. By Conjecture 2.23, approximately 99.999981% of all totally real quintic fields conjecturally have $\rho_\infty \neq 4$. Thus, we expect that cyclic quintic fields with $\rho_\infty = 0$ must be quite abundant. Note, however, that cyclic quintic fields are a subset of density 0 among all totally real quintic fields, so the conjectures of Dummit and Voight do not apply directly here.

2.4. **Refinements of the bound on the rank.** Now we are ready to improve the bound in Proposition 2.10. We will continue using the notation of Section 2.2.

Proposition 2.25. *Let p be an odd prime, let $C : y^2 = f(x)$ with $f(x)$ of degree p (and genus $g = (p-1)/2$), such that L, the number field defined by $f(x)$, is totally real of degree p, and let $J/\mathbb{Q}$ be the jacobian of $C/\mathbb{Q}$. Let $\rho_\infty = \dim_{\mathbb{F}_2} \mathcal{O}_L^{\times,+}/(\mathcal{O}_L^\times)^2$, and let $j_\infty = \dim_{\mathbb{F}_2}(\mathrm{res}_\infty(\mathcal{O}_L^\times/(\mathcal{O}_L^\times)^2) \cap J_\infty)$. Then:*

$$\dim \mathrm{Sel}^{(2)}(\mathbb{Q}, J) \leq j_\infty + \rho_\infty + \dim \mathrm{Cl}^+(L)[2] + \dim G \cap \mathrm{val}\left(L_{J_\infty}\right),$$

In particular,

1. *(1)* $\rho_\infty + j_\infty \leq p - 1$.
2. *(2)* $j_\infty \leq \dim J_\infty = (p-1)/2 = \mathrm{genus}(C)$.
3. *(3)* $\dim \mathrm{Cl}^+(L)[2] \leq \rho_\infty + \dim \mathrm{Cl}(L)[2]$. *In particular,*
$$\dim \mathrm{Sel}^{(2)}(\mathbb{Q}, J) \leq j_\infty + 2\rho_\infty + \dim \mathrm{Cl}(L)[2] + \dim G \cap \mathrm{val}\left(L_{J_\infty}\right),$$
4. *(4) If $G \cap \mathrm{val}\left(L_{J_\infty}\right)$ is trivial, then*
$$\dim \mathrm{Sel}^{(2)}(\mathbb{Q}, J) \leq j_\infty + \rho_\infty + \dim \mathrm{Cl}^+(L)[2] \leq j_\infty + 2\rho_\infty + \dim \mathrm{Cl}(L)[2].$$

Proof. Let p be an odd prime, let $C : y^2 = f(x)$ with $f(x)$ of degree p, such that L, the number field defined by $f(x)$, is totally real of degree p, and let $J/\mathbb{Q}$ be the jacobian of $C/\mathbb{Q}$. Recall that in Section 2.1 we showed

$$\begin{aligned}\dim \mathrm{Sel}^{(2)}(\mathbb{Q}, J) &\leq \dim(\widehat{H}) = \dim U + \dim V + \dim W \\ &= \dim\left(\mathcal{O}_L^\times/(\mathcal{O}_L^\times)^2 \cap \mathrm{res}_\infty^{-1}(J_\infty)\right) + \dim \mathrm{Cl}(L_{J_\infty})[2] + \dim G \cap \mathrm{val}\left(L_{J_\infty}\right).\end{aligned}$$

Clearly,

$$\begin{aligned}\dim\left(\mathcal{O}_L^\times/(\mathcal{O}_L^\times)^2 \cap \mathrm{res}_\infty^{-1}(J_\infty)\right) &= \dim \mathrm{res}_\infty(\mathcal{O}_L^\times/(\mathcal{O}_L^\times)^2) \cap J_\infty + \dim \ker(\mathrm{res}_\infty|_{\mathcal{O}_L^\times/(\mathcal{O}_L^\times)^2}) \\ &= j_\infty + \dim \mathcal{O}_L^{\times,+}/(\mathcal{O}_L^\times)^2 = j_\infty + \rho_\infty.\end{aligned}$$

Now, for part (1), notice that $\left(\mathcal{O}_L^\times/(\mathcal{O}_L^\times)^2 \cap \mathrm{res}_\infty^{-1}(J_\infty)\right) \subseteq \mathcal{O}_L^\times/(\mathcal{O}_L^\times)^2$ so the dimension as a $\mathbb{F}_2$-vector space is at most p. Moreover, $\mathrm{res}_\infty(-1)$ is not in J_∞ (because $J_\infty = \delta_\infty(J(\mathbb{R})) \subseteq H_\infty$, which is the kernel of the norm map, so $N_{\mathbb{Q}}^L(j) = 1$ for $j \in L$ such that $\mathrm{res}_\infty(j) \in J_\infty$, but $N_{\mathbb{Q}}^L(-1) = -1$ since the degree of L is odd). Thus, $j_\infty + \rho_\infty = \dim\left(\mathcal{O}_L^\times/(\mathcal{O}_L^\times)^2 \cap \mathrm{res}_\infty^{-1}(J_\infty)\right) \leq p - 1$, as claimed.

For part (2), recall that we have defined $J_\infty = \delta_\infty(J(\mathbb{R})/2J(\mathbb{R})) \subseteq H_\infty$. By Lemma 2.9, and the fact that δ_∞ is injective (Lemma 4.1 in [22]), we have

$$\dim(J_\infty) = m_\infty - 1 - g = p - 1 - \frac{p-1}{2} = \frac{p-1}{2},$$

where we have used the fact that L is totally real to claim that $m_\infty = p$.

Part (3) follows from Theorem 2.13, which shows that $\rho^+ \leq \rho_\infty + \rho$. And part (4) is immediate from (3), so the proof is complete. □

Now we can put together Corollary 2.15 and Proposition 2.25 to give a bound in the cases when the multiplicative order of 2 mod p is even.

Theorem 2.26. *Suppose L is a cyclic number field of degree $p > 2$, such that the order of 2 in $(\mathbb{Z}/p\mathbb{Z})^\times$ is even. Then, in the notation of Proposition 2.25, we have*

$$\begin{aligned}\dim \mathrm{Sel}^{(2)}(\mathbb{Q}, J) &\leq j_\infty + \rho_\infty + \dim \mathrm{Cl}(L)[2] + \dim \ker \big(G \to \mathrm{Cl}(L)/2\mathrm{Cl}(L)\big) \\ &\leq p - 1 + \dim \mathrm{Cl}(L)[2] + \dim \ker \big(G \to \mathrm{Cl}(L)/2\mathrm{Cl}(L)\big).\end{aligned}$$

Moreover, if $\rho_\infty = 0$, then

$$\begin{aligned}\dim \mathrm{Sel}^{(2)}(\mathbb{Q}, J) &\leq g + \dim \mathrm{Cl}(L)[2] + \dim \ker \big(G \to \mathrm{Cl}(L)/2\mathrm{Cl}(L)\big) \\ &= \frac{p-1}{2} + \dim \mathrm{Cl}(L)[2] + \dim \ker \big(G \to \mathrm{Cl}(L)/2\mathrm{Cl}(L)\big).\end{aligned}$$

Proof. Suppose L is a cyclic number field of degree $p > 2$, such that the order of 2 in $(\mathbb{Z}/p\mathbb{Z})^\times$ is even. Then, Corollary 2.15 implies that $\rho = \rho^+$. Thus, the bound follows from Proposition 2.25. □

3. Genus 1

The goal of this section is to show an alternative proof of Theorem 1.1, using Stoll's implementation of the 2-descent algorithm and the results we showed in the previous section. Let m be an integer such that $D = m^2 + 3m + 9$ is square-free and not divisible by 3. Let C be the (hyper)elliptic curve given by the Weierstrass equation

$$C : y^2 = f_m(x) = x^3 + mx^2 - (m+3)x + 1.$$

Since C is elliptic, the jacobian J is isomorphic to C, so we will identify C with J. We will conclude the bound stated in the theorem as a consequence of Theorem 2.26. Since the order of $2 \equiv -1 \bmod 3$ is 2, Corollary 2.15 shows that $\rho^+ = \rho$. In Section 2.3 we discussed that cyclic cubic fields with $\rho_\infty \neq 0$ are rare. Let us show that in fact $\mathcal{O}_L^{\times,+} = (\mathcal{O}_L^\times)^2$, and therefore $\rho_\infty = 0$, for the cyclic cubic fields $L = L_m$ defined by $f_m(x) = 0$.

Lemma 3.1 ([23, §1, p. 371])**.** *Let m be an integer such that $m \equiv 3 \bmod 9$, and let L be the number field defined by $f_m(x) = x^3 + mx^2 - (m+3)x + 1 = 0$. Then, $\rho_\infty = 0$.*

Proof. Let α be the negative root of $f_m(x)$. Then $\alpha' = 1/(1-\alpha)$, and $\alpha'' = 1 - 1/\alpha$ are the two other roots, and in fact they are units in $\mathcal{O}_L^\times$. Moreover,

$$-m - 2 < \alpha < -m - 1 < 0 < \alpha' < 1 < \alpha'' < 2$$

and therefore all eight possible sign signatures may obtained from α and its conjugates. Thus, every totally positive unit is a square, and $\rho_\infty = 0$, as claimed. □

Thus, in order to prove Theorem 1.2, it is enough to show that G is trivial.

Lemma 3.2. *Let $m \geq 0$ be an integer such that $D = m^2 + 3m + 9$ is square-free and not divisible by 3. Let $v = 2$, or let v be a prime divisor of D, and let $f_m(x) = x^3 + mx^2 - (m+3)x + 1$. Then, $f_m(x)$ is irreducible as a polynomial in $\mathbb{Q}_v[x]$.*

Proof. Let $v = 2$. Then, if we consider $f_m(x)$ as a polynomial in $\mathbb{F}_2[x]$, we have

$$f_m(x) = \begin{cases} x^3 + x^2 + 1 & \text{if } m \equiv 1 \mod 2, \\ x^3 + x + 1 & \text{if } m \equiv 0 \mod 2. \end{cases}$$

In both cases, f_m is irreducible over $\mathbb{F}_2$, hence it is irreducible over $\mathbb{Q}_2$.

Now, let $v > 2$ be a prime divisor of D. Then, by assumption, $v > 3$ and

$$f_m(x - m/3) = x^3 - \frac{D}{3}x + \frac{D \cdot (2m+3)}{27}$$

is integral over $\mathbb{Z}_v$. Since $D = m^2 + 3m + 9$, it follows that $4D - (2m+3)^2 = 27$ and therefore the greatest common divisor of D and $2m + 3$ divides 27. Since by assumption D is not divisible by 3, then $\gcd(D, 2m+3) = 1$; this together with the fact that D is square-free implies that $f_m(x - m/3)$ is Eisenstein over $\mathbb{Z}_v$. Hence, f_m is irreducible over $\mathbb{Q}_v$, as claimed. □

We are now ready to prove Theorem 1.1.

Theorem 3.3 ([23, Theorem 1])**.** *Let $m \geq 0$ be an integer such that $m^2 + 3m + 9$ is square-free and not divisible by 3. Let E_m be the elliptic curve given by the Weierstrass equation*

$$E_m : y^2 = f_m(x) = x^3 + mx^2 - (m+3)x + 1.$$

Let L_m be the number field generated by a root of $f_m(x)$, and let $\mathrm{Cl}(L_m)$ be its class group. Then,

$$\mathrm{rank}_{\mathbb{Z}}(E_m(\mathbb{Q})) \leq 1 + \dim_{\mathbb{F}_2}(\mathrm{Cl}(L_m)[2]).$$

Proof. We shall use Theorem 2.26. The order of $2 \equiv -1 \bmod 3$ is 2, even, so $\rho = \rho^+$, and Lemma 3.1 shows that $\rho_\infty = 0$, so it remains to compute $G_m = \prod_{v \in S_m \setminus \{\infty\}} G_{m,v}$.

The discriminant of f_m is $D^2 = (m^2 + 3m + 9)^2$, so we have

$$S_m = \{\infty, 2\} \cup \{v \mid D\}.$$

However, by Lemma 3.2, the polynomial $f_m(x)$ is irreducible over $\mathbb{Q}_v$ for any finite prime $v \in S_m$. It follows that the number of irreducible factors of $f_m(x)$ over $\mathbb{Q}_v$ is 1, and therefore $I_{m,v}$ is zero-dimensional by Lemma 2.7. Since $G_{m,v} \subseteq I_{m,v}$, we conclude that $G_{m,v}$ is always trivial. Hence, G_m is trivial, and Theorem 2.26 implies that

$$\dim \mathrm{Sel}^{(2)}(\mathbb{Q}, J_m) \leq g + \dim \mathrm{Cl}(L_m)[2] + \dim \ker\left(G_m \to \mathrm{Cl}(L_m)/2\mathrm{Cl}(L_m)\right) = g + \dim \mathrm{Cl}(L_m)[2],$$

where J_m is the jacobian of the elliptic curve E_m. Since the genus of E_m is 1, then $E_m \cong J_m$ over $\mathbb{Q}$. Moreover, $f_m(x)$ is irreducible over $\mathbb{Q}$, and therefore the 2-torsion $E(\mathbb{Q})[2]$ is trivial. Hence,

$$\mathrm{rank}_{\mathbb{Z}}(E_m(\mathbb{Q})) \leq \dim \mathrm{Sel}^{(2)}(\mathbb{Q}, E_m) \leq 1 + \dim \mathrm{Cl}(L_m)[2],$$

as desired. □

4. Genus 2

In this section we apply Stoll's implementation of 2-descent as described in Section 2 to prove that the jacobians of a certain family of hyperelliptic curves of genus 2 have Selmer rank bounded *only* in terms of the class group of the field of definition of the 2-torsion points. The family of hyperelliptic curves that we discuss here arises from a family of degree 5 cyclic extensions of $\mathbb{Q}$ described by Lehmer in [13], in section 5, which we describe next. For every $n \in \mathbb{N}$, we let

$$f_n(x) = x^5 + n^2x^4 - 2(n^3 + 3n^2 + 5n + 5)x^3 + (N - 4n^2 - 10n - 20)x^2 + (n^3 + 4n^2 + 10n + 10)x + 1$$

with

$$N(n) = n^4 + 5n^3 + 15n^2 + 25n + 25.$$

Then, f_n defines a cyclic extension of $\mathbb{Q}$. Further, the discriminant of f_n is given by

$$\operatorname{disc}(f_n) = h(n)^2 N(n)^4,$$

where $h(n) = n^3 + 5n^2 + 10n + 7$. In fact, if t is a rational number such that $f_t(x)$ is irreducible, then we still have that $f_t(x)$ defines a cyclic extensions of $\mathbb{Q}$ of degree 5. Thus, thinking about $f_t(x)$ as taking a rational parameter gives us a full 1-parameter family of cyclic extensions of $\mathbb{Q}$. We will consider the hyperelliptic curve $C_t : y^2 = f_t(x)$ for some well chosen $t \in \mathbb{Q}$ so that $\operatorname{disc}(f_t)$ is exactly a rational 4th power. However, since $f_t(x)$ is not integral for $t \in \mathbb{Q}$, we find an integral model for C_t as follows. Let $t = a/b$ with relatively prime integers a, b and consider $f_{a/b}(x)$. The least common denominator of the coefficients of $f_{a/b}(x)$ is b^4, therefore the polynomial

$$\begin{aligned} g_{a,b}(x) &= f_{a/b}\left(\frac{x}{b^4}\right) b^{20} \\ &= x^5 + a^2b^2x^4 + (-2a^3b^5 - 6a^2b^6 - 10ab^7 - 10b^8)x^3 + (a^4b^8 + 5a^3b^9 + 11a^2b^{10} \\ &\quad + 15ab^{11} + 5b^{12})x^2 + (a^3b^{13} + 4a^2b^{14} + 10ab^{15} + 10b^{16})x + b^{20} \end{aligned}$$

is integral and monic. Moreover, note that $C_t : y^2 = f_t(x)$ and $C_{a,b} : y^2 = g_{a,b}(x)$ are isomorphic over $\mathbb{Q}$ via the map $(x, y) \mapsto (b^4x, b^{10}y)$. Further, since $\operatorname{disc}(f_t) = (t^3 + 5t^2 + 10t + 7)^2N^4$, then

$$\operatorname{disc}(g_{a,b}(x)) = b^{80} \cdot \operatorname{disc}(f_{a/b}(x)) = b^{80} \cdot h(a/b)^2 \cdot N(a/b)^4.$$

Hence, $\operatorname{disc}(g_{a,b})$ is a 4th power exactly when t is a rational number such that $h(t) = t^3+5t^2+10t+7$ is a square in $\mathbb{Q}$. In other words, $\operatorname{disc}(g_{a,b})$ is a 4th power if there is a point $P = (t, s)$ on the elliptic curve $E : Y^2 = X^3 + 5X^2 + 10X + 7$. The elliptic curve $E/\mathbb{Q}$ has Cremona label `368e1`, rank 1, and trivial torsion subgroup over $\mathbb{Q}$. Since the rank of E over $\mathbb{Q}$ is positive, we know that there are infinitely many specializations of $t = a/b \in \mathbb{Q}$ such that the discriminant of $g_{a,b}(x)$ is a 4th power, as desired. With this choice of t values, our goal is to prove the following theorem.

Theorem 4.1. *Let $E : Y^2 = X^3 + 5X^2 + 10X + 7$, let $P = (-1, -1) \in E(\mathbb{Q})$ be the generator of the Mordell-Weil group of E, let $n \geq 1$ be an integer congruent to 1 or 5 mod 6, and let $t = t_n = x(nP)$ be the x-coordinate of nP. Let $f_t(x)$ be as above and let $L_t/\mathbb{Q}$ be the cyclic degree 5 Galois extension defined by adjoining a root of $f_t(x)$. Let C_t be the hyperelliptic curve cut out by the equation $y^2 = f_t(x)$ with jacobian J_t (equivalently, C_t is defined by $y^2 = g_{a,b}(x)$ where $t = a/b$ in lowest terms). Then,*

$$\operatorname{rank}_{\mathbb{Z}}(J_t) \leq j_\infty + \rho_\infty + \dim_{\mathbb{F}_2} \operatorname{Cl}(L_t)[2] + 4 \cdot \mu_5(N(t))$$

where $\mu_5(N(t))$ is the number of prime divisors v of the numerator of $N(t)$ such that $\nu_v(N(t)) \equiv 0 \bmod 5$, and $j_\infty + \rho_\infty \leq 4$. Moreover, if $\rho_\infty = 0$, then

$$\operatorname{rank}_{\mathbb{Z}}(J_t) \leq 2 + \dim_{\mathbb{F}_2} \operatorname{Cl}(L_t)[2] + 4 \cdot \mu_5(N(t)).$$

To prove the theorem, we apply the process of 2-descent described in Section 2 for C_t, but instead we use the isomorphic model $C_{a,b} : y^2 = g_{a,b}(x)$ since $g_{a,b}$ has been constructed specifically to be monic and integral so that [22] applies. We will only need to carry out steps 1 and 2 of the descent in order to compute G, and then we will apply Theorem 2.26, to conclude the theorem. The proof will be put together in Section 4.3.

Remark 4.2. As one would expect, it is rare to encounter a value of t such that $\mu_5(N(t)) > 0$. In fact, if $n \equiv 1$ or $5 \bmod 6$ with $1 \leq n \leq 17$, and $t = x(nP)$ as in statement of Theorem 4.1, then a Magma computation shows that $\mu_5(N(t)) = 0$. Note, however, in general there are values of t such that $N(t)$ has a prime factor p such that $\nu_p(N(t)) \equiv 0 \bmod 5$. For instance, $N(7721) = 11^5 \cdot 26501 \cdot 833201$, so $\mu_5(N(7721)) = 1$, but 7721 is not the x-coordinate of a point nP as above.

Remark 4.3. Since $g_{a,b}(x) = f_{a/b}(x/b^4)b^{20}$, both polynomials f_t and $g_{a,b}$ define the same extension $L_t/\mathbb{Q}$. We will continue to denote by $L_{t,p}$ the algebra over $\mathbb{Q}_p$ as in Stoll notation, that is defined by either of the polynomials f_t or $g_{a,b}$. Notice that $L_t/\mathbb{Q}$ is a cyclic Galois extension of degree 5, so $L_{t,p}$ is either an extension of degree 5 of $\mathbb{Q}_p$, or the product of five copies of $\mathbb{Q}_p$.

4.1. **Step 1.** Recall that we have computed

$$\begin{aligned}\operatorname{disc}(g_{a,b}(x)) &= b^{80} \cdot \operatorname{disc}(f_{a/b}(x)) \\ &= b^{80} \cdot h(a/b)^2 \cdot N(a/b)^4, \\ &= b^{58} \cdot (b^3 h(a/b))^2 \cdot (b^4 N(a/b))^4,\end{aligned}$$

where now

$$\mathcal{H}(a,b) = b^3 h(a/b) = a^3 + 5a^2 b + 10ab^2 + 7b^3$$

and

$$\mathcal{N}(a,b) = b^4 N(a/b) = a^4 + 5a^3 b + 15a^2 b^2 + 25ab^3 + 25b^4$$

are integers relatively prime to b, since $\gcd(a,b) = 1$. Thus,

$$S_t = \{\infty, 2\} \cup \big\{v \text{ prime} : v \mid \operatorname{disc}(g_{a,b})\big\} = \{\infty, 2, v \mid b\} \cup \{v \mid \mathcal{H}(a,b)\} \cup \{v \mid \mathcal{N}(a,b)\},$$

and continue on to step 2.

4.2. **Step 2.** The goal of this step is to compute the group $G_t = \prod_{v \in S_t \setminus \{\infty\}} G_{t,v} \subseteq I(L_t)/I(L_t)^2$ and, in fact, prove that the component $G_{t,v}$ is trivial for most $v \in S_t \setminus \{\infty\}$. Recall that $m_{t,v}$ is the number of factors in the factorization of $g_{a,b}(x)$ over $\mathbb{Q}_v$. In particular, if $m_{t,v} = 1$, then $I_{t,v}$ is trivial by Lemma 2.7, and therefore $G_{t,v} = \operatorname{val}_p(J_{t,v}) \subseteq I_{t,v}$ must be trivial as well.

Since $S_t = \{\infty, 2, v \mid b\} \cup \{v \mid \mathcal{H}(a,b)\} \cup \{v \mid \mathcal{N}(a,b)\}$, we will consider several cases according to what factor of the discriminant v divides (and we will treat $v = 2$ and 5 separately).

4.2.1. *Case of $v = 2$.* Recall that we have chosen t to be the x-coordinate of a point $Q = nP$, where $P = (-1,-1)$ is a generator of $E(\mathbb{Q}) \cong \mathbb{Z}$, and $n \equiv 1$ or $5 \bmod 6$. Since $(-1,-1) \equiv (1,1) \bmod 2$ is non-singular on $\widetilde{E}/\mathbb{F}_2$, and $\widetilde{E}^{\mathrm{ns}}(\mathbb{F}_2)$, the group of non-singular points over $\mathbb{F}_2$, contains two points ($(1,1)$ and $\mathcal{O}$), it follows that if n is odd, then $x(nP) \equiv 1 \bmod 2$, and in particular, the denominator of $x(nP)$ is not even. Thus, if $t = x(nP) = a/b$ written as a fraction in reduced terms, then b is odd.

If we reduce

$$\begin{aligned}g_{a,b}(x) = x^5 + a^2b^2x^4 + (-2a^3b^5 - 6a^2b^6 - 10ab^7 - 10b^8)x^3 + (a^4b^8 + 5a^3b^9 + 11a^2b^{10} \\ + 15ab^{11} + 5b^{12})x^2 + (a^3b^{13} + 4a^2b^{14} + 10ab^{15} + 10b^{16})x + b^{20}\end{aligned}$$

modulo 2, then we obtain either

$$g_{a,b}(x) \equiv \begin{cases} x^5 + x^2 + 1 & \text{if } a \equiv 0 \bmod 2, \\ x^5 + x^4 + x^2 + x + 1 & \text{if } a \equiv 1 \bmod 2. \end{cases}$$

Since both polynomials are irreducible over $\mathbb{F}_2$ and $g_{a,b}(x)$ is integral and monic, it follows that $g_{a,b}(x)$ is irreducible over $\mathbb{Q}_2$. Hence $m_{t,2} = 1$, and I_2 is trivial. Since $G_{t,2} \subseteq I_2$, we conclude that $G_{t,2}$ is trivial as well.

4.2.2. *Case of $v = 5$.* If we reduce

$$g_{a,b}(x) = x^5 + a^2b^2x^4 + (-2a^3b^5 - 6a^2b^6 - 10ab^7 - 10b^8)x^3 + (a^4b^8 + 5a^3b^9 + 11a^2b^{10} + 15ab^{11} + 5b^{12})x^2 + (a^3b^{13} + 4a^2b^{14} + 10ab^{15} + 10b^{16})x + b^{20}$$

modulo 5, for all possible values of a and b mod 5, we find that $g_{a,b}(x)$ is irreducible, unless

$$(a, b) \equiv (1, 3),\ (2, 1),\ (3, 4),\ \text{or } (4, 2) \bmod 5.$$

However, notice that $t = x(nP)$ is an x-coordinate of a rational point on an elliptic curve in Weierstrass form $Y^2 = h(X)$, with h cubic and monic, therefore the denominator b of t must be a perfect square, and thus congruent to 0, 1, or 4 mod 5. If $(a, b) \equiv (2, 1)$ or $(3, 4) \bmod 5$, then $x(nP) = t = a/b \equiv 2 \bmod 5$. Now, $P \equiv (4, 4) \bmod 5$ generates $\widetilde{E}(\mathbb{F}_5)$, which is cyclic of order 6, and $x(nP) \equiv 2 \bmod 5$ if and only if $n \equiv 3 \bmod 6$. Since n was chosen to be 1 or 5 mod 6, it follows that $x(nP) \not\equiv 2 \bmod 5$, and therefore $(a, b) \not\equiv (2, 1)$ nor $(3, 4) \bmod 5$, and it follows that $g_{a,b}(x)$ is irreducible over $\mathbb{F}_5$ and $\mathbb{Q}_5$.

Hence, $m_{t,5} = 1$ and I_5 is trivial, which implies that $G_{t,5}$ is trivial as well.

Remark 4.4. One can go into more detail and show that, in fact, the pair $(a, b) \equiv (3, 4) \bmod 5$ does not happen for any x-coordinate $x(nP) = a/b$, but we do not need this here.

4.2.3. *Primes that divide $\mathcal{N}(a, b)$.* First suppose that v is an odd prime, dividing $\operatorname{disc}(g_{a,b})$, and such that v is inert or ramified in $L_t/\mathbb{Q}$ (note that if v ramifies, then it is totally ramified because $L_t/\mathbb{Q}$ is Galois of prime degree). In this case, the v-adic extension $L_{t,v}/\mathbb{Q}_v$ is unramified or totally ramified, respectively, of degree 5, and therefore $g_{a,b}(x)$ must be irreducible over $\mathbb{Q}_v$, because $g_{a,b}(x)$ and $f_t(x)$ both define $L_{t,v}$. In particular, $m_{t,v} = 1$ and therefore $G_{t,v}$ is trivial as explained in the first paragraph of Step 2. We need the following lemma.

Lemma 4.5. *Let $v \neq 2, 5$ be a prime that divides $\mathcal{N} = \mathcal{N}(a, b)$, such that $\nu_v(\mathcal{N})$ is not a multiple of 5. Then, v ramifies in $L_t/\mathbb{Q}$, where $t = a/b$.*

Proof. Let $v \neq 2, 5$ be a prime that divides $\mathcal{N}(a, b)$. Since $\mathcal{N}(a, b)$ and b are relatively prime (as noted above in Step 1), it follows that $\nu_v(N(a/b)) > 0$. Considering $t \in \mathbb{Q}_v$, the polynomial $f_t(x)$ (and also $g_{a,b}(x)$) describes the local algebra $L_{t,v}$ over $\mathbb{Q}_v$, so it suffices to show that the roots of $f_t(x)$ have fractional valuation to prove that $L_{t,v}/\mathbb{Q}_v$ defines a totally ramified extension of degree 5, and therefore v ramifies in $L_t/\mathbb{Q}$.

Let us define $\tilde{f}_t(x) = f_t(x - t^2/5)$. It follows that f_t and $\tilde{f}_t$ defined the same algebra $L_{t,v}$, and $\tilde{f}_t$ is still monic, and integral over $\mathbb{Q}_v$ (recall that $\nu_v(b) = 0$ and $v \neq 5$). Then, $\tilde{f}_t(x)$ is given by

$$\tilde{f}_t(x) = x^5 + a_3(t)x^3 + a_2(t)x^2 + a_1(t)x + a_0(t),$$

where the $a_i(t)$ are polynomials in t that factor as follows:

$$a_3 = N(t),\ a_2 = N(t) \cdot (t^2 + 5/2t + 5/4),\ a_1 = N(t) \cdot (t^4 + 5t^3 + 20/3t^2 - 50/3)$$

and

$$a_0 = N(t) \cdot \left(t^6 + \frac{15}{2}t^5 + \frac{65}{4}t^4 - 50t^2 - \frac{125}{4}t + \frac{125}{4}\right).$$

We claim that the v-adic valuation of $b_0(t) = a_0(t)/N(t)$ is 0. Indeed, Euclid's algorithm yields polynomials

$$x(t) = \frac{12}{3125}t^5 + \frac{58}{3125}t^4 + \frac{3}{625}t^3 - \frac{26}{625}t^2 - \frac{7}{125}t + \frac{8}{125}$$

and

$$y(t) = -\frac{12}{3125}t^3 - \frac{28}{3125}t^2 - \frac{16}{625}t - \frac{12}{625},$$

such that

$$x(t) \cdot N(t) + y(t) \cdot b_0(t) = 1.$$

Since $v \neq 2, 5$, we have $x(t)$, $y(t)$, $N(t)$, and $b_0(t) \in \mathbb{Z}_v$, and $\nu_v(N) > 0$ implies that $\nu_v(b_0) = 0$, as claimed.

Now, let $m = \nu_v(N) > 0$ and recall that we are assuming that $m \not\equiv 0 \bmod 5$. Then, the Newton polygon of

$$\tilde{f}_t^*(x) = \frac{\tilde{f}_t(x)}{a_0(t)} = 1 + \frac{a_1(t)}{a_0(t)}x + \cdots + \frac{1}{a_0(t)}x^5$$

is given by a single line from $(0, 0)$ to $(5, -m)$. Thus, $\tilde{f}_t^*(x)$ (and therefore $\tilde{f}_t(x)$), has 5 roots of valuation $m/5$ which is not an integer by our hypothesis. We conclude that the extension $L_{t,v}$ over $\mathbb{Q}_v$ defined by $\tilde{f}_t(x)$ (and also by $f_t(x)$) is totally ramified of degree 5, as we needed. □

In particular, by Lemma 4.5, if v divides $\mathcal{N}(a, b)$, and the valuation is not a multiple of 5, then $G_{t,v}$ is trivial. Otherwise, for each of those primes v such that the valuation of $\mathcal{N}$ at v is a positive multiple of 5, the group $G_{t,v}$ may be at most $(m_{t,v} - 1)$-dimensional (where $m_{t,v} \leq 5$), and therefore they may contribute up to $4\mu_5(\mathcal{N}(a, b))$ to the dimension of the kernel of $G \to \mathrm{Cl}(L)/2\mathrm{Cl}(L)$.

4.2.4. *Primes that divide $\mathcal{H}(a, b)$.* Now suppose that v is an odd prime divisor of $\mathcal{H}(a, b)$. In this case, we shall see that $J_v = \delta_v(J(\mathbb{Q}_v))$ is non-trivial, but $G_v = \mathrm{val}_v(J_v)$ is trivial. We shall use Lemma 2.5 to describe J_v and the definition of the val_v map to show that G_v vanishes. Note that $\dim J(\mathbb{Q}_v)/2J(\mathbb{Q}_v) = \dim J(\mathbb{Q}_v)[2]$ by Lemma 2.7 (because $v \neq 2$). Thus, $\delta_v(J(\mathbb{Q}_v))$, is generated by $\delta_v(P_j)$ where $P_1, \ldots, P_{m_{t,v}-1}$ are generators of the 2-torsion $J(\mathbb{Q}_v)[2]$. The values $\delta_v(P_j)$ are given by Lemma 2.5, and in order to compute these values, we need a bit more information about the roots of $f_t(x)$ over $\mathbb{Q}_v$.

If v is inert or ramified in $L_t/\mathbb{Q}$, then $g_{a,b}(x)$ is irreducible over $\mathbb{Q}_v$, and so $m_{t,v} = 1$ and G_v is trivial. Thus, we shall assume that v splits completely in $L_t/\mathbb{Q}$ and therefore $g_{a,b}(x)$ splits completely in $\mathbb{Q}_v[x]$. Recall that b and $\mathcal{H}(a, b) = b^3h(a/b) = a^3 + 5a^2b + 10ab^2 + 7b^3$ are relatively prime, because $\gcd(a, b) = 1$. Since we are assuming that v divides $\mathcal{H}(a, b)$, it follows that v does not divide b and v divides $h(a/b)$. Further, $g_{a,b}(x) = f_t(x/b^4)b^{20}$, hence the roots $\{\alpha_i\}_{i=1}^5$ of $g_{a,b}$ and the roots $\{\beta_i\}_{i=1}^5$ of f_t over $\mathbb{Q}_v$ differ by a unit (namely $\alpha_i = b^4\beta_i$ for all $1 \leq i \leq 5$), so we will work with $f_t(x)$ instead, where $t = a/b \in \mathbb{Z}_v$. If we consider $f_t(x)$ as a polynomial in $(\mathbb{Z}[t])[x]$ for the time being, and reduce the coefficients modulo $h(t)$, then $f_t(x)$ factors as follows over $(\mathbb{Z}[t]/(h(t))[x]$:

$$f_t(x) \equiv (x - (t - 1)) \cdot (x - (t - 2)) \cdot (x - (t^2 + 4t + 5)) \cdot (x + (t^2 + 3t + 4))^2 \bmod h(t)\mathbb{Z}[x].$$

Therefore, if $\beta_1, \ldots, \beta_5$ are the roots of $f_t(x)$ in $\mathbb{Q}_v$, then there are two roots, say β_4 and β_5, such that $\beta_4 \equiv \beta_5 \equiv -(t^2 + 3t + 4) \bmod v$, because $\nu_v(h(t)) = \nu_v(\mathcal{H}(a, b)) > 0$. Further, we note that

$$(t^3 + 5t^2 + 10t + 18)h(t) - (t^2 + 5t + 5)N(t) = 1$$

is an identity in $\mathbb{Z}[t]$. It follows that if $\nu_v(h(t)) > 0$, then $\nu_v(N(t)) = 0$.

Recall that we have chosen $t \in \mathbb{Q}$ such that $h(t)$ is a square. In other words, t is the X-coordinate of a rational point on the elliptic curve $Y^2 = h(X)$. Thus, if $\nu_v(h(t)) > 0$, then the valuation is even. Suppose $\nu_v(h(t)) = 2k > 0$. Then, the v-adic valuation of $\mathrm{disc}(f_t(x))$ is given by

$$\nu_v(\mathrm{disc}(f_t(x))) = \nu_v(h(t)^2 \cdot N(t)^2) = \nu_v(h(t)^2) + \nu_v(N(t)^2) = 2\nu_v(h(t)) + 2\nu_v(N(t)) = 4k,$$

since $\nu_v(h(t)) = 2k$ and $\nu_v(N(t)) = 0$. Since β_4 and β_5 are congruent roots modulo $h(t)\mathbb{Z}_v$, it follows that $\nu_v(\beta_4 - \beta_5) = 2k$ also. Moreover, no other roots can be congruent modulo v, because if another pair was congruent, say $\beta_i \equiv \beta_j \bmod v$, with $\{i, j\} \neq \{4, 5\}$, then

$$\nu_v(\mathrm{disc}(f_t(x))) = \nu_v\left(\prod_{1 \leq i < j \leq 5} (\beta_i - \beta_j)^2\right) \geq 4k + 2,$$

but we saw the valuation is $4k$. Thus, the only roots of $f_t(x)$ that are congruent modulo v are β_4 and β_5. Since $\alpha_i = b^4\beta_i$, we conclude that the only roots of $g_{a,b}(x)$ that are congruent modulo v are α_4 and α_5, and $\nu_v(\alpha_4 - \alpha_5) = \nu_v(\beta_4 - \beta_5) = 2k$ is even.

Now we are ready to resume our computation of $\delta_v(J_t(\mathbb{Q}_v))$. Let $P_j = (\alpha_j, 0)$, for $1 \leq j \leq 5$ be the 2-torsion points on $J(\mathbb{Q}_v)$, and let $L_{t,v} = L_{t,v,1} \times \cdots \times L_{t,v,5} \cong (\mathbb{Q}_v)^5$ where $L_{t,v,j}$ is the copy of $\mathbb{Q}_v$ corresponding to the factor $(x - \alpha_j)$ of $f_t(x)$. Recall that we had set up notation $L_{t,v} = \mathbb{Q}_v[\theta]$, where θ is the image of T under the reduction map $\mathbb{Q}_v[T] \to \mathbb{Q}_v[T]/(f_t(T))$. In particular, $\theta = \alpha_i$ in $L_{t,v,i}$. In the notation of Lemma 2.5, we have $g_{a,b}(x) = f_1(x)h_1(x)$ with $f_1(x) = x - \alpha_1$ and $h_1(x) = (x - \alpha_2) \cdots (x - \alpha_5)$, and

$$\delta_K(P_j) = (-1)^{\deg(f_j)} f_j(\theta) + (-1)^{\deg(h_j)} h_j(\theta) \bmod (L_K^\times)^2.$$

Thus, the image of P_i via δ_v is given by

$$\begin{aligned}
\delta_v(P_1) &= ((\alpha_1 - \alpha_2)(\alpha_1 - \alpha_3)(\alpha_1 - \alpha_4)(\alpha_1 - \alpha_5),\ \alpha_1 - \alpha_2,\ \alpha_1 - \alpha_3,\ \alpha_1 - \alpha_4,\ \alpha_1 - \alpha_5),\\
\delta_v(P_2) &= (\alpha_2 - \alpha_1,\ (\alpha_2 - \alpha_1)(\alpha_2 - \alpha_3)(\alpha_2 - \alpha_4)(\alpha_2 - \alpha_5),\ \alpha_2 - \alpha_3,\ \alpha_2 - \alpha_4,\ \alpha_2 - \alpha_5),\\
&\vdots\\
\delta_v(P_5) &= (\alpha_5 - \alpha_1,\ \alpha_5 - \alpha_2,\ \alpha_5 - \alpha_3,\ \alpha_5 - \alpha_4,\ (\alpha_5 - \alpha_1)(\alpha_5 - \alpha_2)(\alpha_5 - \alpha_3)(\alpha_5 - \alpha_4)).
\end{aligned}$$

Since $G_{t,v} = \mathrm{val}_p(J_v)$, and $J_v = \delta_v(J_t(\mathbb{Q}_v))$ is generated by the values $\delta_v(P_i)$, we compute $\mathrm{val}_v(\delta_v(P_i))$. Recall that $I_v = \ker(N\colon I_v(L_t)/I_v(L_t)^2 \to I(\mathbb{Q})/I(\mathbb{Q})^2)$ and $\mathrm{val}_v\colon H_v \to I_v$ is the map induced by the valuations on each component of $L_{t,v}$. Moreover, by our work above, the only roots that are

congruent modulo v are α_4 and α_5, and $\nu_v(\alpha_4-\alpha_5)=2k$. Thus,

$$\begin{aligned}
\mathrm{val}_p v(\delta_v(P_1)) &= \mathrm{val}_v((\alpha_1-\alpha_2)(\alpha_1-\alpha_3)(\alpha_1-\alpha_4)(\alpha_1-\alpha_5),\ \alpha_1-\alpha_2,\ \alpha_1-\alpha_3,\ \alpha_1-\alpha_4,\ \alpha_1-\alpha_5)\\
&= ((1),\ (1),\ (1),\ (1),\ (1)),\\
\mathrm{val}_v(\delta_v(P_2)) &= \mathrm{val}_v(\alpha_2-\alpha_1,\ (\alpha_2-\alpha_1)(\alpha_2-\alpha_3)(\alpha_2-\alpha_4)(\alpha_2-\alpha_5),\ \alpha_2-\alpha_3,\ \alpha_2-\alpha_4,\ \alpha_2-\alpha_5)\\
&= ((1),\ (1),\ (1),\ (1),\ (1)),\\
\mathrm{val}_v(\delta_v(P_3)) &= ((1),\ (1),\ (1),\ (1),\ (1)),\\
\mathrm{val}_v(\delta_v(P_4)) &= \mathrm{val}_v(\alpha_4-\alpha_1,\ \alpha_4-\alpha_2,\ \alpha_4-\alpha_3,\ (\alpha_4-\alpha_1)(\alpha_4-\alpha_2)(\alpha_4-\alpha_3)(\alpha_4-\alpha_5),\ \alpha_4-\alpha_5)\\
&= ((1),\ (1),\ (1),\ (p)^{2k},\ (p)^{2k}) \equiv ((1),\ (1),\ (1),\ (1),\ (1)) \bmod I(\mathbb{Q})^2,\\
\mathrm{val}_p(\delta_p(P_5)) &= \mathrm{val}_p(\alpha_5-\alpha_1,\ \alpha_5-\alpha_2,\ \alpha_5-\alpha_3,\ \alpha_5-\alpha_4,\ (\alpha_5-\alpha_1)(\alpha_5-\alpha_2)(\alpha_5-\alpha_3)(\alpha_5-\alpha_4))\\
&= ((1),\ (1),\ (1),\ (p)^{2k},\ (p)^{2k}) \equiv ((1),\ (1),\ (1),\ (1),\ (1)) \bmod I(\mathbb{Q})^2.
\end{aligned}$$

Hence, $G_{t,v}=\mathrm{val}_v(J_v)$ must be trivial.

4.2.5. *Primes that divide b.* Suppose that v is an odd divisor of b, where $t=a/b$, and recall that we have chosen t to be the X-coordinate of a rational point $(X_0,Y_0)\in E(\mathbb{Q})$ on the elliptic curve $E/\mathbb{Q}: Y^2=h(X)$. The denominator of $t=X_0$ is therefore a perfect square ($h(X)$ is a monic cubic polynomial), and it follows that $\nu_v(b)=2k>0$ for some $k\geq 1$.

The polynomial $g_{a,b}(x)$ is given by

$$\begin{aligned}
g_{a,b}(x) &= f_{a/b}\left(\frac{x}{b^4}\right)b^{20}\\
&= x^5+a^2b^2x^4+(-2a^3b^5-6a^2b^6-10ab^7-10b^8)x^3+(a^4b^8+5a^3b^9+11a^2b^{10}\\
&\quad +15ab^{11}+5b^{12})x^2+(a^3b^{13}+4a^2b^{14}+10ab^{15}+10b^{16})x+b^{20}.
\end{aligned}$$

We define $g^*_{a,b}(x)=b^{-20}g_{a,b}(x)\in\mathbb{Q}_v[x]$. Then,

$$\begin{aligned}
g^*_{a,b}(x) &= 1+b^{-7}(a^3+4a^2b+10ab^2+10b^3)x+b^{-12}(a^4+5a^3b+11a^2b^2+15ab^3+5b^4)x^2\\
&\quad +b^{-15}(-2a^3-6a^2b-10ab^2-10b^3)x^3+a^2b^{-18}x^4+b^{-20}x^5.
\end{aligned}$$

Since a and b are relatively prime integers, and taking into account that the valuation of b is $2k$, it follows that the Newton polygon of $g^*_{a,b}(x)$ has vertices

$$(0,0),\ (1,-14k),\ (2,-24k),\ (3,-30k),\ (4,-36k),\ (5,-40k),$$

and slopes $-14k$, $-10k$, $-6k$ (length of segment is 2), and $-4k$. Therefore, there are single roots of valuation $\nu_v(\alpha_1)=4k$, $\nu_v(\alpha_2)=10k$, and $\nu_v(\alpha_3)=14k$, and two roots of valuation $\nu_v(\alpha_4)=\nu_v(\alpha_5)=6k$. In order to investigate the valuation of $\alpha_4-\alpha_5$ further, let us put $\alpha_j=b^3\alpha'_j$ and $g'(x)=g^*_{a,b}(b^3x)$ so that α'_j for $j=4,5$ are roots of g' of valuation 0. Thus,

$$\begin{aligned}
g'(x) &= 1+b^{-4}(a^3+4a^2b+10ab^2+10b^3)x+b^{-6}(a^4+5a^3b+11a^2b^2+15ab^3+5b^4)x^2\\
&\quad +b^{-6}(-2a^3-6a^2b-10ab^2-10b^3)x^3+a^2b^{-6}x^4+b^{-5}x^5.
\end{aligned}$$

The vertices are now $(0,0)$, $(1,-4)$, $(2,-6)$, $(3,-6)$, $(4,-6)$, $(5,-5)$ so, indeed, there exactly two roots of zero valuation, namely α_4' and α_5'. By considering $b^6 g'(x)$, we see that

$$\begin{aligned} b^6 g'(x) = (a^4 + 5a^3b + 11a^2b^2 + 15ab^3 + 5b^4)x^2 + (-2a^3 - 6a^2b - 10ab^2 - 10b^3)x^3 + a^2x^4 \\ + b \cdot (b^5 + b(a^3 + 4a^2b + 10ab^2 + 10b^3)x + x^5), \end{aligned}$$

and since $g'(\alpha_j') = 0$, we discover that α_j' is a root of

$$x^2a^2(x-a)^2 + b\hat{g}'(x) = 0,$$

for some polynomial $\hat{g}'(x) \in \mathbb{Z}_v[x]$. Therefore $\alpha_j' \equiv a \bmod v^k$ for $j = 4, 5$. In fact, let us now consider $\alpha_j = b^3\alpha_j' = b^3(a + \alpha_j''b)$ and $g''(x) = g'(a + bx)$. Then, $b^4 g''(x)$ is of the form

$$a^4(2 - 3x + x^2) + b\hat{g}''(x),$$

for some polynomial $\hat{g}''(x) \in \mathbb{Z}_v[x]$. It follows that $\alpha_j'' \equiv 1$ or $2 \bmod v^{2k}$. Hence, we conclude that

$$\alpha_j \equiv b^3(a + b(1 + \kappa_1 b)) \text{ or } b^3(a + b(2 + \kappa_2 b),$$

for some $\kappa_i \in \mathbb{Z}_v$. Thus,

$$\alpha_5 - \alpha_4 = b^4(1 + (\kappa_2 - \kappa_1)b)$$

is of valuation $\nu_v(\alpha_5 - \alpha_4) = \nu_v(b^4) = 8k$, even. Hence, the valuation of all differences $\alpha_i - \alpha_j$ for $1 \le i < j \le 5$ is even.

Therefore, we can compute $\mathrm{val}_v(\delta_v(P_i))$ as in Section 4.2.4 and conclude that these values are trivial in I_v, for all $1 \le i \le 5$, because we are working modulo squares of ideals. Hence, $G_{t,v}$ is trivial.

4.3. **Proof of Theorem 4.1.** By our work on Steps 1 and 2 above, we have shown that $G_{t,v}$ is trivial for all primes $v \ge 2$, except, perhaps, for those primes v such that v^5 divides $\mathcal{N}(a,b)$. If $G_{t,v}$ is non-trivial, then its dimension is at most that of I_v, which is $m_{t,v} - 1 \le 4$. Therefore, the dimension of $G = \prod_{v \in S_t \setminus \{\infty\}} G_{t,v}$ is at most $4 \cdot \mu_5(\mathcal{N}(a,b))$, where $\mu_5(m)$ is the number of distinct prime divisors of the numerator of $m \in \mathbb{Q}$ such that $\nu_v(m) \equiv 0 \bmod 5$. Since v cannot divide $\mathcal{N}(a,b)$ and v simultaneously, and $\mathcal{N}(a,b) = b^4 N(t)$, then $\mu_5(\mathcal{N}(a,b)) = \mu_5(N(t))$. In particular,

$$\dim(\ker(G \to \mathrm{Cl}(L_t)/2\mathrm{Cl}(L_t))) \le \dim G \le 4 \cdot \mu_5(N(t)).$$

Since the extension $L/\mathbb{Q}$ is cyclic of degree 5, and the order of $2 \bmod 5$ is 4, even, we can apply Theorem 2.26 to show

$$\begin{aligned} \dim \mathrm{Sel}^{(2)}(\mathbb{Q}, J) &\le j_\infty + \rho_\infty + \dim \mathrm{Cl}(L)[2] + \dim \ker \big(G \to \mathrm{Cl}(L)/2\mathrm{Cl}(L)\big) \\ &\le j_\infty + \rho_\infty + \dim \mathrm{Cl}(L)[2] + 4 \cdot \mu_5(N(t)), \end{aligned}$$

as claimed. And if in addition we have $\rho_\infty = 0$, then

$$\dim \mathrm{Sel}^{(2)}(\mathbb{Q}, J) \le 2 + \dim \mathrm{Cl}(L)[2] + 4 \cdot \mu_5(N(t)),$$

since $(p-1)/2 = 2$. This concludes the proof of Theorem 4.1.

5. Genus $g = (p-1)/2$, where p is a Sophie Germain prime

The goal of this section is to find examples of hyperelliptic curves of genus $g > 2$ where the dimension of the Selmer group can be bounded in terms of a class group, as in Theorem 1.1 (genus 1 case) or Theorem 4.1 (genus 2 case). We begin by looking at polynomials $f(x)$ that cut out extensions of degree p, contained inside a q-th cyclotomic extension, where q is another prime.

Theorem 5.1. *Let $q > 2$ be a prime such that the multiplicative order of $2 \bmod q$ is either $q-1$ or $(q-1)/2$, and let $p > 2$ be a prime dividing $q-1$. Let $\mathbb{Q}(\zeta_q)$ be the q-th cyclotomic field, and let L be the unique extension of degree p contained in $\mathbb{Q}(\zeta_q)$. Further, suppose that $\mathcal{O}_L = \mathbb{Z}[\alpha]$ for some algebraic integer $\alpha \in L$, let $f(x)$ be the minimal polynomial of α, and let $J/\mathbb{Q}$ be the jacobian variety associated to the hyperelliptic curve $C : y^2 = f(x)$. Then,*

$$\dim \mathrm{Sel}^{(2)}(\mathbb{Q}, J) \leq \rho_\infty + g + \dim \mathrm{Cl}^+(L)[2].$$

If in addition the multiplicative order of $2 \bmod p$ is even, then

$$\dim \mathrm{Sel}^{(2)}(\mathbb{Q}, J) \leq \rho_\infty + g + \dim \mathrm{Cl}(L)[2].$$

Proof. We apply Stoll's algorithm to $y^2 = f(x)$, in order to compute G. Note that $f(x)$ is monic, integral, and irreducible over $\mathbb{Q}$, since α generates $\mathcal{O}_L$ as a ring. Moreover, since $\mathcal{O}_L = \mathbb{Z}[\alpha]$, it also follows that

$$\mathrm{disc}(f(x)) = \mathrm{disc}(\mathcal{O}_L),$$

and since $L \subseteq \mathbb{Q}(\zeta_q)$, the only prime dividing $\mathrm{disc}(\mathcal{O}_L)$ is q. Hence, the set $S = \{\infty, 2, q\}$. We will show that G_2 and G_q are trivial, and therefore G is trivial as well. Indeed:

- Let $v = 2$. Since the order of 2 modulo q is $q-1$ or $(q-1)/2$ by hypothesis, it follows from [15, Theorem 26] that 2 splits into 1 or 2 prime ideals in $\mathbb{Z}(\zeta_q)/\mathbb{Z}$, and therefore 2 must be inert in the intermediary extension $L/\mathbb{Q}$ of degree p. In particular, the polynomial $f(x)$ is irreducible over $\mathbb{Q}_2$, since it defines an unramified extension $L_2/\mathbb{Q}_2$ of degree p. Hence, $m_2 = 1$, and the dimension of I_2 is $m_2 - 1 = 0$ by Lemma 2.7. Since $G_2 \subseteq I_2$, we conclude that G_2 is trivial as well.
- Let $v = q$. Since $L \subseteq \mathbb{Q}(\zeta_q)$ and q is totally ramified in the cyclotomic extension, it is also totally ramified in $L/\mathbb{Q}$. Thus, $f(x)$ is irreducible over $\mathbb{Q}_q$ because it defines a totally ramified extension $L_q/\mathbb{Q}_q$ of degree p. Thus, $m_q = 1$ and arguing as above in the case of $v = 2$, we conclude that G_q is trivial.

Since the only finite primes in S are 2 and q, it follows that $G = G_2 \times G_q$ is trivial. Now, Proposition 2.25 shows the bound $\dim \mathrm{Sel}^{(2)}(\mathbb{Q}, J) \leq \rho_\infty + g + \dim \mathrm{Cl}^+(L)[2]$. If in addition the order of 2 mod p is even, and since $L/\mathbb{Q}$ is cyclic of degree p, then Corollary 2.15 shows that $\rho = \rho^+$. Hence $\dim \mathrm{Sel}^{(2)}(\mathbb{Q}, J) \leq \rho_\infty + g + \dim \mathrm{Cl}(L)[2]$, as claimed. □

The drawback, however, of the previous result is that there are very few subfields of cyclotomic extensions with a power basis, as the following result points out.

Theorem 5.2 (Gras, [10])**.** *Let L be an extension of degree $p \geq 5$, and let $\mathcal{O}_L$ be the maximal order of L. Then, $\mathcal{O}_L$ has a power basis if and only if $L = \mathbb{Q}(\zeta_q)^+$ is the maximal real subfield of the q-th cyclotomic field, where q is a prime with $q = 2p + 1$.*

For instance, the unique cyclic number field of degree 5 with a power basis for the maximal order is $\mathbb{Q}(\zeta_{11})^+$. Also, there is no cyclic number field of degree 7 with a power basis for its maximal order

(since 15 is not a prime). Hence, we concentrate on those cyclic extensions of degree p, where p is a Sophie Germain prime, i.e., $q = 2p + 1$ is also prime.

Theorem 5.3. *Let $q \geq 7$ be a prime such that $p = (q-1)/2$ is also prime, and let $L = \mathbb{Q}(\zeta_q)^+$ be the maximal real subfield of $\mathbb{Q}(\zeta_q)$. Let $f(x) \in \mathbb{Z}[x]$ be any monic integral polynomial defining L, let $C : y^2 = f(x)$, and let $J/\mathbb{Q}$ be its jacobian. Then,*

$$\dim \mathrm{Sel}^{(2)}(\mathbb{Q}, J) \leq \rho_\infty + j_\infty + \dim \mathrm{Cl}^+(L)[2] + \dim \ker \big(G \to \mathrm{Cl}(L)/2\mathrm{Cl}(L)\big).$$

Moreover, if $f(x)$ is the minimal polynomial of $\zeta_q + \zeta_q^{-1}$ or $-(\zeta_q + \zeta_q^{-1})$, then

$$\dim \mathrm{Sel}^{(2)}(\mathbb{Q}, J) \leq \rho_\infty + j_\infty + \dim \mathrm{Cl}^+(L)[2].$$

Further, if one of the following conditions is satisfied,

1. *the Davis–Taussky conjecture holds, or*
2. *the prime 2 is inert in the extension $\mathbb{Q}(\zeta_p)^+/\mathbb{Q}$,*
3. *$q \leq 92459$,*

then $\rho_\infty = 0$, and $\dim \mathrm{Sel}^{(2)}(\mathbb{Q}, J) \leq g + \dim \mathrm{Cl}(L)[2]$.

Proof. The first bound follows from Proposition 2.25, so let us assume that $f(x)$ is the minimal polynomial of $\zeta_q + \zeta_q^{-1}$ or $-(\zeta_q + \zeta_q^{-1})$. The ring of integers $\mathcal{O}_{\mathbb{Q}(\zeta_q)^+}$ has a power basis, namely $\mathbb{Z}[\zeta_q + \zeta_q^{-1}]$. Moreover, since p is a Sophie Germain prime (with $q = 2p + 1$ prime), it follows that the multiplicative order of 2 mod q is a divisor of $2p = 2 \cdot ((q-1)/2)$. Since $q \geq 7$, the order of 2 is bigger than 2, so it must be $p = (q-1)/2$ or $q - 1$. Thus, Theorem 5.1 applies and we obtain $\dim \mathrm{Sel}^{(2)}(\mathbb{Q}, J) \leq \rho_\infty + j_\infty + \dim \mathrm{Cl}^+(L)[2]$.

Further, if (1), (2), or (3) holds, then by Conjecture 2.19, or Theorem 2.18, respectively, we find that $\rho_\infty = 0$ and $\rho = \rho^+$.

If $q \leq 92459$, we shall use the computational approach at the end of Section 2.2 to show that $\rho_\infty = 0$. Let $\zeta = \zeta_q = e^{2\pi i/q}$. Then, the ring of integers of $\mathbb{Q}(\zeta_q)^+$ has a power basis, namely $\mathcal{O}_{\mathbb{Q}(\zeta_q)^+} = \mathbb{Z}[\zeta_q + \zeta_q^{-1}]$. Let $u = -(\zeta + \zeta^{-1})$ if $p \equiv 1 \bmod 4$ and $u = \zeta + \zeta^{-1}$ if $p \equiv 3 \bmod 4$, thus chosen so that u is a unit in $\mathcal{O}_L^\times$ of norm 1. Moreover, we note that if $p \equiv 1 \bmod 4$, then

$$-(\zeta+\zeta^{-1}) < -(\zeta^2+\zeta^{-2}) < \cdots < -(\zeta^{\frac{p-1}{2}}+\zeta^{-\frac{p-1}{2}}) < 0 < -(\zeta^{\frac{p+1}{2}}+\zeta^{-\frac{p+1}{2}}) < \cdots < -(\zeta^p+\zeta^{-p}) < 1,$$

and if $p \equiv 3 \bmod 4$, then

$$\zeta^p + \zeta^{-p} < \zeta^{p-1} + \zeta^{-(p-1)} < \cdots < \zeta^{\frac{p+1}{2}} + \zeta^{-\frac{p+1}{2}} < 0 < \zeta^{\frac{p-1}{2}} + \zeta^{-\frac{p-1}{2}} < \cdots < \zeta + \zeta^{-1} < 1.$$

Thus, according to our conventions described in this section, the embeddings $\tau_1, \ldots, \tau_p$ are numbered so that $\tau_i(u) = r_i \in \mathbb{R}$ with

$$r_i = \begin{cases} -(\zeta^i + \zeta^{-i}) & \text{if } p \equiv 1 \bmod 4, \\ \zeta^{p+1-i} + \zeta^{-(p+1-i)} & \text{if } p \equiv 3 \bmod 4, \end{cases}$$

for all $1 \leq i \leq p$. Thus,

$$\mathrm{res}_\infty(u) = (-1, -1, -1, \ldots, 1, 1, 1) \in H_\infty$$

with $(p-1)/2$ minus ones when $p \equiv 1 \bmod 4$, and $(p+1)/2$ minus ones when $p \equiv 3 \bmod 4$.

Now, the Galois group $\mathcal{G} = \mathrm{Gal}(L/\mathbb{Q})$ is cyclic of order p. Since $q = 2p + 1$ is prime, then the multiplicative order of 2 mod q is $(q-1)/2$ or $q - 1$. Thus, either -2 or 2 is a primitive root mod q. Let $\gamma\colon L \to L$ that sends $\gamma(\zeta) = \zeta^2$. It follows that $\sigma = \overline{\gamma} \in \mathcal{G} \cong (\mathbb{Z}/q\mathbb{Z})^\times/\{\pm 1\}$ is a generator.

Thus, the automorphism $\sigma(\zeta+\zeta^{-1}) = \zeta^2+\zeta^{-2}$ generates $\mathcal{G}$. Let $\phi = \phi_\sigma \in S_p$ be the permutation attached to σ as defined above. For instance, if $p \equiv 1 \bmod 4$, then $r_1 = -(\zeta+\zeta^{-1})$, where $\zeta = e^{2\pi i/q}$, so $\tau_1(\sigma(u)) = r_2 = -(\zeta^2+\zeta^{-2})$ and therefore $\phi(1) = 2$. However, if $p \equiv 3 \bmod 4$, then $r_1 = \zeta^p+\zeta^{-p}$. We can find an integer $1 \leq k \leq p$, and k or $-k \equiv 2p \bmod q$, such that $\sigma(u) = \zeta^k+\zeta^{-k}$. It follows that $\tau(\sigma(u)) = r_k$ and so $\phi(1) = k$ in this case. In general, the permutation ϕ is defined by

$$\phi(i) = \min\{2\cdot i \bmod q,\ (-2\cdot i) \bmod q\}$$

when $p \equiv 1 \bmod 4$, and by

$$\phi(i) = p+1-\min\{(2\cdot(p+1-i)) \bmod q,\ q-(2\cdot(p+1-i) \bmod q)\},$$

when $p \equiv 3 \bmod 4$, where our representatives in $\mathbb{Z}/q\mathbb{Z}$ are always chosen amongst $\{0,1,\ldots,q-1\}$. With these explicit descriptions of $\mathrm{res}_\infty(u)$ and ϕ_σ, we have computed (using Magma) the matrix $M_{\infty,u}$ for all primes p and q, with $q \leq 92459$, as in the statement, and in all cases $d_{\infty,u} = p-1$. Hence, $\rho_\infty = 0$ follows from Lemma 2.21. □

Remark 5.4. If the Davis–Taussky conjecture holds, then the class number h_K of $\mathbb{Q}(\zeta_q)$ is odd (by Theorem 2.20), and therefore the class number h_K^+ of $L = \mathbb{Q}(\zeta_q)^+$ is odd as well (because h_K^+ is a divisor of h_K). Hence, if the Davis–Taussky conjecture holds, then $\mathrm{Cl}(L)[2]$ is trivial, and the bound of Theorem 5.3 becomes

$$\dim \mathrm{Sel}^{(2)}(\mathbb{Q}, J) \leq g.$$

6. Examples

6.1. **Curves of Genus 1.** In this section we present some data that was collected on the curves described in Theorem 1.1 (the data collected can be found at [4]). For $m \in \mathbb{Z}$, let $f_m(x)$, E_m, and L_m be as in Theorem 1.1. Using Magma, we attempted to compute (subject to GRH) the Mordell–Weil rank of $E_m(\mathbb{Q})$ and $\dim_{\mathbb{F}_2} \mathrm{Cl}(L_m)[2]$ for every $m \in \mathbb{Z}$ such that $1 \leq m \leq 20000$ and m^2+3m+9 is both square-free and not divisible by 3. There are 12462 such values of m in the given interval, and we were able to compute the rank of $E_m/\mathbb{Q}$ for 12235 of them. For the other 227 curves, we were only able to get upper and lower bounds on their rank.

Of the 12462 curves that we tested, 10327 of them (about 82.87%) had rank equal to the upper bound given in Theorem 1.1. However, one might expect that the sharpness of this upper bound would decay as m gets larger and larger, and in fact that seems to be the case. Let us define a function to keep track of the sharpness of the bound in an interval.

Definition 6.1. *Let*

$$M = \{m \in \mathbb{Z} : 1 \leq m \leq 20000 \text{ and } m^2+3m+9 \text{ is both square-free and not divisible by } 3\}$$

and $S = \{m \in M : \mathrm{rank}\,(E_m) = \dim \mathrm{Cl}(L_m)+1\}$. *Given* $I \subseteq M$, *we define* $\mathrm{Sharp}(I) = \dfrac{\#(S \cap I)}{\#(M \cap I)}$.

Remark 6.2. The set S only includes curves whose rank was actually computable and, because of this, the $\mathrm{Sharp}(I)$ statistic only gives a lower bound for how sharp Washington's upper bound is over the set I.

In order to see how the sharpness of the upper bound degrades as m grows, in Table 1 we present $\mathrm{Sharp}(I)$ over disjoint intervals of length 1000. In the data, we clearly see that the number of curves for which Washington's bound is sharp in a given interval does start to decrease, but the bound is

I	Sharp(I)	I	Sharp(I)
$[1, 1000]$	0.91451	$[10001, 11000]$	0.81862
$[1001, 2000]$	0.88499	$[11001, 12000]$	0.81451
$[2001, 3000]$	0.87581	$[12001, 13000]$	0.79936
$[3001, 4000]$	0.84665	$[13001, 14000]$	0.81833
$[4001, 5000]$	0.82051	$[14001, 15000]$	0.81760
$[5001, 6000]$	0.82504	$[15001, 16000]$	0.78560
$[6001, 7000]$	0.84911	$[16001, 17000]$	0.82664
$[7001, 8000]$	0.84455	$[17001, 18000]$	0.82258
$[8001, 9000]$	0.81862	$[18001, 19000]$	0.80512
$[9001, 10000]$	0.80000	$[19001, 20000]$	0.78583

TABLE 1. Measure of the sharpness of the bound presented in Theorem 1.1.

b	$\#(T(1) \cap B(b))$	$\#(T(3) \cap B(b))$	$\#(T(5) \cap B(b))$	$\#(T(7) \cap B(b))$	$\frac{\#(T(b) \cap B(b))}{\#B(b)}$
1	7391	0	0	0	1.0000
3	1565	2809	0	0	0.6422
5	37	298	125	0	0.2717
7	0	1	7	2	0.2000
Totals	8993	3108	132	2	——

TABLE 2. Sharpness for a fixed rank bound b in the interval $1 \leq m \leq 20000$.

still sharp more often than not (notice, however, that the sharpness is inflated by the fact that the bound is sharp every time the bound is 1, since there is a point of infinite order $P = (0, 1)$ on E_m).

To see how fixing the bound first affects its sharpness, we define the following sets

$$T(r) = \{m \in M : \operatorname{rank}(E_m) = r\} \text{ and } B(b) = \{m \in M : \dim \mathrm{Cl}(L_m)[2] + 1 = b\}.$$

In Table 2, for each bound b that occurs we give the number of curves of rank r whose bound is b for each r that occurs. We also give the percentage of the curves whose rank is exactly b and provide the totals of each column so that we can see how many curves of each rank we found (for similar statistics and conjectures in a broader context, see [14]).

From Table 2 we can see that all of the curves that we computed, have odd rank less than or equal to 7. It also turns out that for all of the curves that we computed, Washington's bound is also odd and less than or equal to 7. In Table 3, we give the first m such that $\operatorname{rank}(E_m) = r$ and $\dim \mathrm{Cl}(L_m) + 1 = b$ for each pair (r, b) that occurred.

It is also interesting to point out that the average rank among curves with $b = 1$ is 1, the average rank among curves with $b = 3$ is 2.23, among curves with $b = 5$ is 3.38, and among curves with $b = 7$ the average rank is 5.20 (see [14] for other examples of *Selmer bias* in genus 1).

m	(r,b)	m	(r,b)	m	(r,b)
1	$(1,1)$	11	$(3,3)$	143	$(5,5)$
170	$(1,3)$	157	$(3,5)$	3461	$(5,7)$
2330	$(1,5)$	19466	$(3,7)$	12563	$(7,7)$

TABLE 3. The first occurrence of each (rank, bound) pair that occurs for some $m \leq 20000$.

Example 6.3. Lastly, for the sake of concreteness, we end this section with an explicit example. When $m = 143$ we have that

$$E_{143} : y^2 = x^3 + 143x^2 - 146x + 1$$

with conductor $2^2 \cdot 20887^2$. Using Magma, we can compute that

$$\mathrm{Cl}(L_{143}) \cong \mathbb{Z}/2\mathbb{Z} + \mathbb{Z}/2\mathbb{Z} + \mathbb{Z}/4\mathbb{Z} + \mathbb{Z}/4\mathbb{Z},$$

and so Washington's bound for the Mordell–Weil rank is $\dim \mathrm{Cl}(L_{143})[2] + 1 = 4 + 1 = 5$. Looking for points on E_{143} we find 5 independent points of infinite order that generate the Mordel–Weil group.

$$E_{143}(\mathbb{Q}) \cong \mathbb{Z}^5 = \langle (126/121, -3023/1331), (90, -1369), (65/64, 577/512), (21/4, -461/8), (-1, 17) \rangle.$$

6.2. **Curves of Genus 2.** In this section we show some examples of hyperelliptic curves of genus 2 that arise from Theorem 1.2, a.k.a. Theorem 4.1. Recall that the curves $C_t/\mathbb{Q}$ that appear in Theorem 4.1 are parametrized by values of $t = t_n = x(nP)$, where $P = (-1, -1)$ is a generator of the Mordell–Weil group over $\mathbb{Q}$ of $E : Y^2 = X^3 + 5X^2 + 10X + 7$, and $n \equiv 1$ or $5 \bmod 6$.

Example 6.4. Let $t_1 = -1$. This value of t corresponds to the curve

$$C_{-1} : y^2 = f_{-1}(x) = x^5 + x^4 - 4x^3 - 3x^2 + 3x + 1.$$

In this case, the field L_{-1} given by $f_{-1}(x)$ is, in fact, the maximal real subfield of $\mathbb{Q}(\zeta_{11})$. Also,

$$N(-1) = 11,$$

thus $\mu_5(N(-1)) = 0$ because no prime in the factorization of 11 appears to a power that is a multiple of 5. Moreover, it is known that $\mathrm{Cl}(L_{-1})$ is trivial (see [24, Tables, §3]).

Thus, Theorem 1.2 says that $\mathrm{rank}_{\mathbb{Z}}(J_{-1}(\mathbb{Q})) \leq 2$, where J_{-1} is the jacobian of C_{-1}. In fact, as we shall prove in Section 6.3, the rank of $J_{-1}(\mathbb{Q})$ is exactly 2.

Unfortunately, as the following example shows, the computations become unwieldy computer-time consuming even for the next value of t, namely t_5.

Example 6.5. Let $t_5 = -49721/123201$. This value of t corresponds to the curve $C_{t_5} : y^2 = f_{t_5}(x)$ where $f_{t_5}(x)$ is given by

$$x^5 + \frac{2472177841}{15178486401}x^4 - \frac{12734762191724324}{1870004703089601}x^3 - \frac{85238319763}{15178486401}x^2 + \frac{12248531781778603}{1870004703089601}x + 1.$$

The value of $N(t)$ at $t_5 = -49721/123201$ is

$$N(t_5) = \frac{3928450255234102524091}{230386449425341932801},$$

and the factorization of the numerator is $11 \cdot 4441 \cdot 79621 \cdot 1009997205221$. Thus, $\mu_5(N(t_5)) = 0$.

Unfortunately, the discriminant of L_{t_5} is so large that we have not been able to compute $\mathrm{Cl}(L_{t_5})$ numerically (the discriminant of L_{t_5} has 118 digits). As a consequence, our computers are also unable to compute the rank of the jacobian of C_{t_5}.

Remark 6.6. The only example of a value of t for Theorem 1.2 where we can compute all invariants is $t_1 = -1$. In all other cases, as illustrated by the previous example, we cannot compute the class group nor the rank of the jacobian. We have been able to compute the value of $\mu_5(N(t_n))$ for $n = 1, 5, 7, 11, 13$, and 17. But already for $n = 19$, the numerator of $N(t_{19})$ has 313 digits and our computers are unable to factor it.

Example 6.7. It is worth pointing out that the conditions on t given in Theorem 1.2 are necessary for the bound of $\operatorname{rank}_{\mathbb{Z}}(J(\mathbb{Q})) \leq 2 + \dim_{\mathbb{F}_2}(\mathrm{Cl}(L)[2]) + 4\mu_5(N(t))$ to hold (of course, the bound given by Proposition 2.25 still holds).

For instance, consider the values $t = 2$ and $t = 4$:

- Let $t = 2$. Then,
$$C\colon y^2 = x^5 + 4x^4 - 70x^3 + 135x^2 + 54x + 1$$
and we have $\dim_{\mathbb{F}_2}(\mathrm{Cl}(L)[2]) = 0$, and $N(2) = 191$ (prime), so that $\mu_5(N(2)) = 0$. A Magma computation shows that $\operatorname{rank}_{\mathbb{Z}}(J(\mathbb{Q})) = 3$.
- Let $t = 4$. Then,
$$C\colon y^2 = x^5 + 16x^4 - 274x^3 + 817x^2 + 178x + 1$$
and we have $\dim_{\mathbb{F}_2}(\mathrm{Cl}(L)[2]) = 4$, and $N(4) = 941$ (prime), so that $\mu_5(N(4)) = 0$. A Magma computation shows that $\operatorname{rank}_{\mathbb{Z}}(J(\mathbb{Q})) = 7$.

Hence, in both cases of $t = 2$ and $t = 4$, the rank of J is one unit higher than the bound produced by Theorem 1.2. Moreover, note that 2 is a primitive root modulo 5, so Theorem 2.14 says that $\rho = \rho^+$, and one can compute that $\rho_\infty = 0$ (using Magma). Hence, Proposition 2.25 says

$$\dim \mathrm{Sel}^{(2)}(\mathbb{Q}, J) \leq j_\infty + \dim \mathrm{Cl}(L)[2] + \dim G \cap \mathrm{val}\,(L_{J_\infty})\,,$$

and we conclude that for $t = 2$ and $t = 4$ we must have that $j_\infty = g = 2$, that G is non-trivial, and we must have $\dim G \cap \mathrm{val}\,(L_{J_\infty}) \geq 1$.

6.3. **Examples in the Sophie Germain case.** In this section we show examples of hyperelliptic curves that arise from Theorem 5.3.

Example 6.8. Let $q = 7$ and $p = 3$. Then, $L = \mathbb{Q}(\zeta_7)^+$ is the maximal real subfield of $\mathbb{Q}(\zeta_7)$, which has degree 3, and class number 1 (see [24, Tables, §3]). Note that the order of 2 in $(\mathbb{Z}/3\mathbb{Z})^\times$ is $2 = p - 1$, and therefore condition (2) of Theorem 5.3 is met. Hence, if $f(x)$ is the minimal polynomial of $\pm(\zeta_7 + \zeta_7^{-1})$, then the jacobian $J(\mathbb{Q})$ of $y^2 = f(x)$ satisfies

$$\operatorname{rank}_{\mathbb{Z}}(J(\mathbb{Q})) \leq \dim_{\mathbb{F}_2} \mathrm{Sel}^{(2)}(\mathbb{Q}, J) \leq g + \dim \mathrm{Cl}(L)[2] = 1.$$

For instance, if $f(x)$ is chosen to be the minimal polynomial of $-(\zeta_7 + \zeta_7^{-1})$, then $f(x) = x^3 - x^2 - 2x + 1$ we in fact recover the elliptic curve E_{-1} of Theorem 1.1 for $m = -1$. The Mordell–Weil rank of the elliptic curve $E_{-1}\colon y^2 = x^3 - x^2 - 2x + 1$ is 1, so the bound on the rank given by Theorem 5.3 in this case is in fact sharp.

Example 6.9. If $q = 11$ and $p = 5$, then $L = \mathbb{Q}(\zeta_{11})^+$ is a field of degree 5 and trivial class group. Since 2 is a primitive root modulo 5, if $f(x)$ be the minimal polynomial of $\pm(\zeta_{11} + \zeta_{11}^{-1})$, then Theorem 5.3 says

$$\operatorname{rank}_{\mathbb{Z}}(J(\mathbb{Q})) \leq \dim_{\mathbb{F}_2} \operatorname{Sel}^{(2)}(\mathbb{Q}, J) \leq g + \dim \operatorname{Cl}(L)[2] = \frac{p-1}{2} = 2,$$

where J is the jacobian of $y^2 = f(x)$. If $f(x)$ is the minimal polynomial of $\zeta_{11} + \zeta_{11}^{-1}$, then $f(x) = x^5 + x^4 - 4x^3 - 3x^2 + 3x + 1$, and we recover the curve C_{-1} of Example 6.4. Below we will describe a general method to find some rational points on the jacobian, and show that $2 \leq \operatorname{rank}_{\mathbb{Z}}(J) \leq 2$. Thus, the rank is 2 and the bound is sharp.

Example 6.10. If $q = 23$ and $p = 11$, then $L = \mathbb{Q}(\zeta_{23})^+$ is a field of degree 11 and trivial class group. Since 2 is a primitive root modulo 11, if $f(x)$ be the minimal polynomial of $\pm(\zeta_{23} + \zeta_{23}^{-1})$, then Theorem 5.3 says

$$\operatorname{rank}_{\mathbb{Z}}(J(\mathbb{Q})) \leq \dim_{\mathbb{F}_2} \operatorname{Sel}^{(2)}(\mathbb{Q}, J) \leq g + \dim \operatorname{Cl}(L)[2] = \frac{p-1}{2} = 5,$$

where J is the jacobian of $y^2 = f(x)$. If $f(x)$ is the minimal polynomial of $-(\zeta_{23} + \zeta_{23}^{-1})$, then

$$f(x) = x^{11} - x^{10} - 10x^9 + 9x^8 + 36x^7 - 28x^6 - 56x^5 + 35x^4 + 35x^3 - 15x^2 - 6x + 1.$$

Below we will show that $4 \leq \operatorname{rank}_{\mathbb{Z}}(J) \leq 5$. A full 2-descent (via Magma) shows that the rank is, in fact, equal to 4.

We finish this section by describing a method to produce points in J (as in Theorem 5.3, and compute the rank of the subgroup generated by these points. Let p be a fixed Sophie Germain prime, let $q = 2p + 1$, and let $L = \mathbb{Q}(\zeta_q)^+$ be the maximal real subfield of $\mathbb{Q}(\zeta_q)$, where ζ_q is a primitive q-th root of unity. The minimal polynomial for $\zeta_q + \zeta_q^{-1}$ has constant term 1 or -1 according to whether p is congruent to 1 or 3 mod 4. If $f \in \mathbb{Z}[x]$ is a polynomial with constant term 1, then the point $(0, 1)$ will be on the curve

$$C : y^2 = f(x)$$

and furthermore the factorization of $f(x) - 1$ will provide points on the jacobian J of C, allowing us to obtain a lower bound for the Mordell–Weil rank of $J(\mathbb{Q})$. For this reason, we define f to be the minimal polynomial of $\theta = (-1)^{(p-1)/2}(\zeta_q + \zeta_q^{-1})$.

A lower bound for the rank can be computed by considering the images of the factors of $f - 1$ in $L^\times/(L^\times)^2$ under the map $\delta_{\mathbb{Q}} : J(\mathbb{Q}) \to H_{\mathbb{Q}}$ (see Section 2). Let $y_0 \in \mathbb{Q}$, let $g(x)$ be an irreducible factor of $f(x) - y_0^2$, and let K be the splitting field of $g(x)$. Then, over K, we have a factorization

$$g(x) = \prod_{i=1}^{n} (x - x_i),$$

and the points $P_i = (x_i, y_0)$ are in $C(K)$. Under the map $\delta_K \colon J(K) \to H_K$, as a map from $C(K)$ to $L_K^\times/(L_K^\times)^2$ we have

$$P_i \mapsto (x_i - \theta_K)(L_K^\times)^2.$$

If f remains irreducible over K, then L_K is simply the composite extension of K and L_q, and $\theta_K = \theta$. As a map from $J(K)$ to $L_K^\times/(L_K^\times)^2$, δ_K is a homomorphism of groups, and hence the divisor

$P_1 + P_2 + \cdots + P_n$ maps to

$$\prod_{i=1}^{n}(x_i - \theta_K)(L_K^\times)^2 = (-1)^n g(\theta_K)(L_K^\times)^2.$$

On the other hand, the divisor $P_1 + P_2 + \cdots + P_n$ can be regarded as the base extension to K of a certain divisor D defined over $\mathbb{Q}$, hence over $\mathbb{Q}$ we have

$$D \mapsto (-1)^n g(\theta)(L^\times)^2,$$

via the map F_K of Section 2. Thus, for each irreducible factor $g(x)$ we obtain a point on the jacobian $J(\mathbb{Q})$ that corresponds to the divisor $D = D(g)$ defined above. Moreover, since the map $J(\mathbb{Q})/2J(\mathbb{Q}) \to H_\mathbb{Q}$ induced by $\delta_\mathbb{Q}$ is injective ([22, Lemma 4.1]), in order to compute the rank of the subgroup generated by $\{D(g)\}_g$, it suffices to check the dimension of the (multiplicative) subgroup generated by $\{\delta_\mathbb{Q}(D(g))\}$ in $H = H_\mathbb{Q}$.

Example 6.11. For example let $q = 11$ and $p = 5$, as in Example 6.9, so $L = \mathbb{Q}(\zeta_{11})^+$ and $f(x) = x^5 + x^4 - 4x^3 - 3x^2 + 3x + 1$. Then, $f(x) - 1$ factors as

$$x(x^2 - 3)(x^2 + x - 1).$$

Their images in $L^\times/(L^\times)^2$ via $\delta_\mathbb{Q}$ are

$$-\theta(L^\times)^2,\ (\theta^2 - 3)(L^\times)^2,\ \text{and}\ (\theta^2 + \theta - 1)(L^\times)^2$$

respectively. To obtain a lower bound for the rank of J it remains only to reduce $\{-\theta, (\theta^2 - 3), (\theta^2 + \theta - 1)\}$ to a multiplicatively independent subset modulo squares. Since the product of all three is

$$-(f(\theta) - 1)(L^\times)^2 = (L^\times)^2$$

we see that at most two are multiplicatively independent. On the other hand $-\theta(\theta^2 - 3)$ is not a square in L, so

$$-\theta(L^\times)^2 \text{ and } (\theta^2 - 3)(L^\times)^2$$

are multiplicatively independent give us a lower bound of 2 as the rank of J over $\mathbb{Q}$. An upper bound of 2 for the rank was computed in Example 6.9, hence the rank is exactly 2.

In Table 4, we have collected the upper bound given by Theorem 5.3, together with some computational data of lower bounds for the rank of the jacobian J associated to the first few Sophie Germain primes, obtained using the method we have described here.

p	5	11	23	29	41	53	83	89	113	131	173
upper	2	5	11	14	20	26	41	44	56	65	86
lower	2	4	6	4	4	4	10	6	4	10	4

TABLE 4. Upper and lower bounds for the rank of $J_q(\mathbb{Q})$ when $p = (q-1)/2$ is Sophie Germain.

References

[1] J. V. Armitage and A. Fröhlich. Classnumbers and unit signatures. *Mathematika*, 14:94–98, 1967. 2.2

[2] Wieb Bosma, John Cannon, and Catherine Playoust. The Magma algebra system. I. The user language. *J. Symbolic Comput.*, 24(3-4):235–265, 1997. Computational algebra and number theory (London, 1993). 1

[3] J. W. S. Cassels. The Mordell-Weil group of curves of genus 2. In *Arithmetic and geometry, Vol. I*, volume 35 of *Progr. Math.*, pages 27–60. Birkhäuser, Boston, Mass., 1983. 2

[4] H. B. Daniels, Á. Lozano-Robledo, and E. Wallace. Data for *Bounds of the rank of the Mordell-Weil group of Jacobians of Hyperelliptic Curves*. Available at https://www3.amherst.edu/~hdaniels/. 6.1

[5] Daniel Davis. Computing the number of totally positive circular units which are squares. *J. Number Theory*, 10(1):1–9, 1978. 2.2, 2.2

[6] D. S. Dummit, J. Voight, and a. w. R. Foote. The 2-Selmer group of a number field and heuristics for narrow class groups and signature ranks of units. *ArXiv e-prints*, January 2017. https://arxiv.org/abs/1702.00092. 1, 2.2, 2.2, 2.3, 2.23

[7] H. M. Edgar, R. A. Mollin, and B. L. Peterson. Class groups, totally positive units, and squares. *Proc. Amer. Math. Soc.*, 98(1):33–37, 1986. 2.2

[8] Dennis R. Estes. On the parity of the class number of the field of qth roots of unity. *Rocky Mountain J. Math.*, 19(3):675–682, 1989. Quadratic forms and real algebraic geometry (Corvallis, OR, 1986). 2.17, 2.2

[9] Dennis A. Garbanati. Unit signatures, and even class numbers, and relative class numbers. *J. Reine Angew. Math.*, 274/275:376–384, 1975. Collection of articles dedicated to Helmut Hasse on his seventy-fifth birthday, III. 2.16, 2.2

[10] M-N. Gras. Non monogénéité de l'anneau des entiers des extensions cycliques de $\mathbf{Q}$ de degré premier $l \geq 5$. *J. Number Theory*, 23(3):347–353, 1986. 5.2

[11] I. Hughes and R. Mollin. Totally positive units and squares. *Proc. Amer. Math. Soc.*, 87(4):613–616, 1983. 2.2

[12] M-H. Kim and S-G. Lim. Square classes of totally positive units. *J. Number Theory*, 125(1):1–6, 2007. 2.2, 2.2

[13] E. Lehmer. Connection between Gaussian periods and cyclic units. *Math. Comp.*, 50(182):535–541, 1988. 1, 4

[14] Á. Lozano-Robledo. A probabilistic model for the distribution of ranks of elliptic curves over $\mathbb{Q}$. *ArXiv e-prints*, November 2016. https://arxiv.org/abs/1611.01999. 6.1, 6.1

[15] D. A. Marcus. *Number fields*. Springer-Verlag, New York-Heidelberg, 1977. Universitext. 5

[16] S. Nakano. A family of quintic cyclic fields with even class number parameterized by rational points on an elliptic curve. *J. Number Theory*, 129(12):2943–2951, 2009. 1

[17] B. Oriat. Relation entre les 2-groupes des classes d'idéaux au sens ordinaire et restreint de certains corps de nombres. *Bull. Soc. Math. France*, 104(3):301–307, 1976. 2.14

[18] B. Poonen and E. F. Schaefer. Explicit descent for Jacobians of cyclic covers of the projective line. *J. Reine Angew. Math.*, 488:141–188, 1997. 2

[19] E. F. Schaefer. 2-descent on the Jacobians of hyperelliptic curves. *J. Number Theory*, 51(2):219–232, 1995. 2

[20] D. Shanks. The simplest cubic fields. *Math. Comp.*, 28:1137–1152, 1974. 1

[21] P. Stevenhagen. Class number parity for the pth cyclotomic field. *Math. Comp.*, 63(208):773–784, 1994. 2.2, 2.2, 2.2

[22] M. Stoll. Implementing 2-descent for Jacobians of hyperelliptic curves. *Acta Arith.*, 98(3):245–277, 2001. 1, 1, 2, 2, 2.4, 2.5, 2.7, 2.8, 2.9, 2.10, 2.1, 2.4, 4, 6.3

[23] L. C. Washington. Class numbers of the simplest cubic fields. *Math. Comp.*, 48(177):371–384, 1987. 1, 1.1, 3.1, 3.3

[24] L. C. Washington. *Introduction to cyclotomic fields*, volume 83 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, second edition, 1997. 6.4, 6.8

Department of Mathematics and Statistics, Amherst College, Amherst, MA 01002, USA
E-mail address: hdaniels@amherst.edu
URL: http://www3.amherst.edu/~hdaniels/

Department of Mathematics, University of Connecticut, Storrs, CT 06269, USA
E-mail address: alvaro.lozano-robledo@uconn.edu
URL: http://alozano.clas.uconn.edu/

Department of Mathematics, University of Connecticut, Storrs, CT 06269, USA
E-mail address: erik.wallace@uconn.edu