Rank stability in quadratic extensions and Hilbert's tenth problem for the ring of integers of a number field

Levent Alpöge, Manjul Bhargava, Wei Ho, and Ari Shnidman

Abstract

We show that for any quadratic extension of number fields K/F, there exists an abelian variety A/F of positive rank whose rank does not grow upon base change to K. This result implies that Hilbert's tenth problem over the ring of integers of any number field has a negative solution. That is, for the ring $\mathcal{O}_K$ of integers of any number field K, there does not exist an algorithm that answers the question of whether a polynomial equation in several variables over $\mathcal{O}_K$ has solutions in $\mathcal{O}_K$.

1 Introduction

In his celebrated 1900 address to the International Congress of Mathematicians, Hilbert [Hil02] discussed 23 major open problems of importance for 20th century mathematics. In particular, his Problem #10 called for an algorithm to determine whether an integer polynomial equation in several variables has solutions in the integers.

Hilbert's 10th problem was answered in the negative by the work of Davis, Putnam, and Robinson [DPR61] and Matiyasevich [Mc70]. The question has since remained whether Hilbert's 10th problem still has a negative answer when the ring of rational integers is replaced by the ring of integers in some number field.

Poonen [Poo02] and independently Cornelissen, Pheidas, and Zahidi [CPZ05] proved that for a number field K, if there exists an elliptic curve defined over $\mathbb{Q}$ with $\operatorname{rank} E(\mathbb{Q}) = \operatorname{rank} E(K) = 1$, then Hilbert's 10th problem has a negative answer for O_K. This was strengthened independently by Poonen and by Shlapentokh [Shl08] to show that the latter condition can be replaced by $\operatorname{rank} E(\mathbb{Q}) = \operatorname{rank} E(K) > 0$. Shlapentokh [MR10, Section 8] also showed that if, for every cyclic extension K/F of prime degree, there exists an elliptic curve E/F such that $\operatorname{rank} E(F) = \operatorname{rank} E(K) > 0$, then Hilbert's tenth problem has a negative solution for the ring of integers of every number field. This was later further strengthened by Shlapentokh [MRS24, Theorems 3.1 and 4.8] to show that if, for every *quadratic* extension K/F of number fields, there exists an *abelian variety* A/F such that $\operatorname{rank} A(F) = \operatorname{rank} A(K) > 0$, then Hilbert's tenth problem has a negative solution for the ring of integers of every number field.

It is the hypothesis of the latter result of Shlapentokh that we prove in this paper:

Theorem 1.1. *Let K/F be any quadratic extension of number fields. Then there exists an abelian variety A/F such that* $\operatorname{rank} A(F) = \operatorname{rank} A(K) > 0$.

Corollary 1.2. *Let K be any number field. Then $\mathbb{Z}$ has a diophantine model over $\mathcal{O}_K$, and so Hilbert's tenth problem has a negative answer over $\mathcal{O}_K$. That is, for the ring $\mathcal{O}_K$ of integers of any number field K, there does not exist an algorithm that answers the question of whether a polynomial equation in several variables over $\mathcal{O}_K$ has solutions.*

Mazur and Rubin [MR10] showed that Corollary 1.2 follows from the conjectural finiteness of the Tate-Shafarevich group; see also the work of Murty and Pasten [**?**] and Pasten [**?**] for two other conditional results. Unconditional proofs for particular classes of number fields were given by a number of authors over the years, including Denef [**?**, **?**], Denef and Lipshitz [**?**], Pheidas [**?**], Shlapentokh [**?**], Videla [**?**], Shapiro–Shlapentokh [**?**], Garcia-Fritz–Pasten [**?**], Shnidman–Weiss [SW23], and Kundu–Lei–Sprung [**?**]. In a beautiful recent preprint, Koymans and Pagano [KP24] give an independent unconditional proof of Corollary 1.2, via a slightly different version of Theorem 1.1, using different methods. However, it is interesting to note that both their proof and ours make use of results in additive combinatorics in number fields, such as the recent work of Kai [Kai23], though in rather different ways.[1]

Finally, we remark that the methods of Koymans and Pagano [KP24] involve 2-Selmer groups of elliptic curves with full 2-torsion over F, while our proof uses ℓ-isogeny Selmer groups of Jacobians J_n of the hyperelliptic curves $C_n : y^2 = x^\ell + n$.

We now describe the ideas behind our proof more precisely. Let ℓ be an odd prime that is unramified in $K = F(\sqrt{q})$, and let ζ denote a primitive ℓ-th root of unity lying in an extension field of K. If $A/F(\zeta)$ is an abelian variety with $\operatorname{rank} A(F(\zeta)) = \operatorname{rank} A(K(\zeta)) > 0$, then we also have $\operatorname{rank} A'(F) = \operatorname{rank} A'(K) > 0$, where A' is the Weil restriction of A from $F(\zeta)$ to F. Thus, for the purposes of proving Theorem 1.1, by replacing K and F by $K(\zeta)$ and $F(\zeta)$, respectively, we may assume without loss of generality that $\zeta \in F$.

We consider the family of curves $C_n : y^2 = x^\ell + n$ where $n \in F$. Their Jacobians J_n admit complex multiplication by ζ over F, and our tool for studying the ranks of these Jacobians J_n is the $(1-\zeta)$-Selmer group. A key realization is that the $(1-\zeta)$-Selmer groups of the abelian varieties J_n admit a large set Σ of *silent primes*, in the terminology of Mazur and Rubin [**?**]; these are the primes of F that are inert or ramified in $F(\sqrt{n})$, and these primes remain silent in that they impose no local conditions in the definition of the said $(1-\zeta)$-Selmer group (see Lemma 2.2).

Using the methods of Mazur–Rubin [MR10] and Yu [Yu16], we choose $n = q^\ell r^2$ so that the Jacobian variety J_n has $(1-\zeta)$-Selmer rank 0 and thus rank 0. We may then replace n by nt^2, with t an arbitrary product of silent primes satisfying a congruence condition modulo a constant depending only on n, and the $(1-\zeta)$-Selmer group of $A := J_n$ will not change (and thus will still vanish!).

This great flexibility in choosing t and thus $n = q^\ell r^2 t^2$ allows us to *simultaneously* also produce a non-torsion rational point on the q-quadratic twist $A^q = J_{r^2t^2}$ of $A = J_{q^\ell r^2 t^2}$, by solving the Σ-unit equation $a + 2rb = 1$. The fact that there are many solutions (a, b) to this Σ-unit equation follows, for example, from a simpler version of Vinogradov's circle method approach to the ternary Goldbach problem [Vin04], as generalized to number fields by Mitsui [Mit60]; it also follows from the recent work of Kai [Kai23]. Once we have such a solution, we obtain an F-rational point on the Fermat curve $ax^\ell + 2ry^\ell = 1$. The latter curve covers $C_{r^2t^2}$, where $t = a^{(\ell-1)/2}b$. In this way, we obtain an F-rational point on the Jacobian $A^q = J_{r^2t^2}$ that is generically non-torsion.

[1] In particular, the case of linear equations in three primes that we use may be considered "classical", in that it can also be deduced from the methods of Vinogradov [Vin04], van der Corput [vdC39], and Mitsui [Mit60, Mit56].

We thereby conclude that

$$\operatorname{rank} A^q(K) = \operatorname{rank} A(F) + \operatorname{rank} A^q(F) = \operatorname{rank} A^q(F) > 0,$$

as desired.

This article is organized as follows. In Section 2, we describe the arithmetic of the curves $C : y^2 = x^\ell + 1$ and their twists, including the definition of the $(1-\zeta)$-Selmer group and its silent primes. We show how to produce an ℓ-ic twist of C having rank 0 using the methods of Mazur–Rubin [MR10] and [Yu16], while ensuring that its further q-quadratic twist has a non-torsion rational point, obtained by making use of a solution to the aforementioned Σ-unit equation where Σ is the set of silent primes. In Section 3, we show how to deduce the existence of infinitely many solutions to the desired Σ-unit equation. Finally, in Section 4, we combine the above ingredients together to prove Theorem 1.1 and thus Corollary 1.2.

> Hello darkness, my old friend
> I've come to talk with you again
> Because a vision softly creeping
> Left its seeds while I was sleeping
> And the vision that was planted in my brain
> Still remains
> Within the sound of silence.
>
> – Simon and Garfunkel

2 The curve $y^2 = x^\ell + 1$ and its twists

Let ℓ be an odd prime, and let F be a number field containing the group μ_ℓ of ℓ-th roots of unity. Let $\zeta \in \mu_\ell$ be a generator. For $n \in F^\times$, let C_n be the smooth projective hyperelliptic curve of genus $(\ell-1)/2$ in weighted projective space $\mathbb{P}(1,(\ell-1)/2,1)$ having affine model $y^2 = x^\ell + n$. Note that for any $\lambda \in F^\times$, the curves C_n and $C_{n\lambda^{2\ell}}$ are isomorphic. The automorphism $(x,y) \mapsto (\zeta x, y)$ induces an action of μ_ℓ on C_n, and hence an action of the ring $\mathbb{Z}[\zeta]$ on the Jacobian $J_n := \operatorname{Jac}(C_n)$.

It will be important for us that the varieties C_n and J_n admit both quadratic twists and μ_ℓ-twists. For a quadratic extension $K = F(\sqrt{q})$ of F, the K-quadratic twist C_n^K of C_n is the curve $qy^2 = x^\ell + n$, which is also isomorphic to $C_{q^\ell n}$. Similarly, the K-quadratic twist J_n^K of J_n is isomorphic to $J_{q^\ell n}$. The μ_ℓ-twists of C_n are the curves C_{nr^2}, for $r \in F^\times$, as C_{nr^2} becomes isomorphic to C_n over $F(r^{1/\ell})$, and the μ_ℓ-twists of J_n are the Jacobians J_{nr^2}.

2.1 $(1-\zeta)$-Selmer groups

Via the embedding $\mathbb{Z}[\zeta] \hookrightarrow \operatorname{End}(J_n)$, we view $1-\zeta$ as a self-isogeny $\phi\colon J_n \to J_n$ of degree ℓ. We study the corresponding Selmer groups $\operatorname{Sel}_\phi(J_n)$ below; see [**?**] for further background on these.

We embed $C \hookrightarrow J$ via $P \mapsto P - \infty$, using the base point $\infty = [1\colon 0\colon 0] \in C_n(F)$. The one-dimensional $\mathbb{F}_\ell$-vector space $J_n[\phi](\overline{F}) = \ker(\phi)(\overline{F})$ is generated by the point $(0, \sqrt{n})$, and the Galois action $\operatorname{Gal}(\overline{F}/F) \to \operatorname{Aut}(J_n[\phi](\overline{F})) \simeq \mathbb{F}_\ell^\times$ on $J_n[\phi]$ is the quadratic character cutting out $F(\sqrt{n})/F$.

Set $T := H^1(F, J_n[\phi])$. For a prime $\mathfrak{p}$, let $F_\mathfrak{p}$ be the corresponding completion of F, and set $T_\mathfrak{p} := H^1(F_\mathfrak{p}, J_n[\phi])$. Let $W_\mathfrak{p} \subset T_\mathfrak{p}$ be the image of the boundary map $J_n(F_\mathfrak{p}) \to T_\mathfrak{p}$ coming from

the short exact sequence

$$0 \to J_n[\phi] \to J_n \xrightarrow{\phi} J_n \to 0. \tag{2.1}$$

The ϕ-Selmer group $\mathrm{Sel}_\phi(J_n)$ is defined to be the kernel of the homomorphism

$$T \to \prod_{\mathfrak{p}} T_{\mathfrak{p}}/W_{\mathfrak{p}}$$

induced by the product of restriction maps $T \to T_{\mathfrak{p}}$. Note that we have ignored the archimedean places, since F is totally complex.

Lemma 2.1. *If* $\mathrm{Sel}_\phi(J_n) = 0$, *then* $\operatorname{rank} J_n(F) = 0$.

Proof. The long exact sequence associated to (2.1) gives $J_n(F)/\phi J_n(F) \hookrightarrow \mathrm{Sel}_\phi(J_n)$, hence the usual Selmer group inequality $\operatorname{rank}_{\mathbb{Z}[\zeta]} J_n(F) \leq \dim_{\mathbb{F}_\ell} \mathrm{Sel}_\phi(J_n)$. □

2.2 Silent primes

Crucial to our method is the presence of so-called *silent primes*, i.e., primes $\mathfrak{p}$ with $T_{\mathfrak{p}} = 0$.

Lemma 2.2. *Suppose* $\mathfrak{p} \nmid \ell$ *is inert or ramified in* $F(\sqrt{n})/F$. *Then* $T_{\mathfrak{p}} = 0$.

Proof. Since F contains μ_ℓ, we see that $J_n[\phi]$ is isomorphic to its own Cartier dual. Hence, local Tate duality gives $H^2(F_{\mathfrak{p}}, J_n[\phi]) \simeq H^0(F_{\mathfrak{p}}, J_n[\phi])$, and the local Euler characteristic formula reads

$$\#T_{\mathfrak{p}} = \#H^0(F_{\mathfrak{p}}, J_n[\phi]) \cdot \#H^2(F_{\mathfrak{p}}, J_n[\phi]) = (\#J_n[\phi](F_{\mathfrak{p}}))^2 = 1.$$

The last equality follows because $\sqrt{n} \notin F_{\mathfrak{p}}$. □

Note that silent primes exist if and only if n is not a square in F.

2.3 Twists of rank zero

Suppose now that $K = F(\sqrt{q})$ is a quadratic extension of F that is unramified at all primes $\mathfrak{p}$ above ℓ. We will consider curves of the form $C_{q^\ell r^2}$ for $r \in \mathcal{O}_F$ and their Jacobians $J_{q^\ell r^2}$. Since $F(\sqrt{q^\ell r^2}) = F(\sqrt{q^\ell})$, we have $J_{q^\ell}[\phi] \simeq J_{q^\ell r^2}[\phi]$, and we may view all Selmer groups $\mathrm{Sel}_\phi(J_{q^\ell r^2})$ as subspaces of the same ambient $\mathbb{F}_\ell$-vector space $T := H^1(F, J_{q^\ell}[\phi])$.

Following the methods of Mazur and Rubin [MR10], Yu [Yu16] proved:

Lemma 2.3 ([Yu16, Theorem 4])**.** *There exists* $r \in \mathcal{O}_F$ *such that* $\mathrm{Sel}_\phi(J_{q^\ell r^2}) = 0$. *Moreover, we may assume that* $r \notin \mathfrak{p}$ *for all primes* $\mathfrak{p}$ *that ramify in* K.

Proof. The first sentence is Yu's theorem, his assumption $\mathrm{Gal}(f) \simeq S_n$ being equivalent to our assumption that q is not a square in $F^\times$. The second sentence is also clear from his proof. □

In the sequel, fix $r \in \mathcal{O}_F$ as in Lemma 2.3. We will use the following notation for special sets of primes in F:

- S' is the set of primes $\mathfrak{p}$ dividing either $\ell!$ or the conductor of $J_{q^\ell r^2}$;
- $S \subset S'$ is the subset of $\mathfrak{p} \in S'$ that are either above ℓ or split in K/F;
- S_{inert} is the infinite set of primes $\mathfrak{p}$ that are inert in K;
- $\Sigma := S \cup S_{\mathrm{inert}}$.

Finally, let $\mathcal{O}_{F,\Sigma}^\times \subset F^\times$ be the set of Σ-units, i.e., those x such that $x \in \mathcal{O}_{F,\mathfrak{p}}^\times$ for all primes $\mathfrak{p} \notin \Sigma$.

Lemma 2.4. *Let $t \in \mathcal{O}_{F,\Sigma}^\times$ and suppose that $t \in F_\mathfrak{p}^{\times \ell}$ for all $\mathfrak{p} \in S$. Then $\mathrm{Sel}_\phi(J_{q^\ell r^2 t^2}) = 0$.*

Proof. The Selmer groups $\mathrm{Sel}_\phi(J_{q^\ell r^2})$ and $\mathrm{Sel}_\phi(J_{q^\ell r^2 t^2})$ live inside the common ambient space T; we will show that their corresponding local conditions $W_\mathfrak{p}$ are equal inside $T_\mathfrak{p}$ for all primes $\mathfrak{p}$. If $\mathfrak{p} \in S$, this is because the two curves are isomorphic over $F_\mathfrak{p}$. Otherwise, if $\mathfrak{p}$ is inert or ramified in K, then $T_\mathfrak{p} = 0$ by Lemma 2.2. In all other cases, we have $\mathfrak{p} \nmid \ell$ and $\mathfrak{p}$ is a prime of good reduction for $J_{q^\ell r^2}$ and $J_{q^\ell r^2 t^2}$, and thus $W_\mathfrak{p} = H^1_{\mathrm{un}}(F_\mathfrak{p}, J_{q^\ell}[\phi])$ for both. Thus $\mathrm{Sel}_\phi(J_{q^\ell r^2 t^2}) = \mathrm{Sel}_\phi(J_{q^\ell r^2}) = 0$. □

2.4 Twists of positive rank

We continue with the assumptions on F and K from §2.3. To produce rational points on certain K-quadratic twists $J_{r^2 t^2}$, we will use solutions to the Σ-unit equation $x + 2ry = 1$. First we need to know that many such solutions exist. For $a, b \in F^\times$, write $t_{a,b} \in F^\times / F^{\times \ell}$ for the class of $a^{\frac{\ell-1}{2}} b$.

Proposition 2.5. *The set*

$$X := \left\{ t_{a,b} : a, b \in \mathcal{O}_{F,\Sigma}^\times, 1 = a + 2rb, a^{\frac{\ell-1}{2}} b \in F_\mathfrak{p}^{\times \ell} \text{ for all } \mathfrak{p} \in S \right\} \subseteq F^\times / F^{\times \ell}$$

is infinite.

Granting Proposition 2.5, whose proof we defer until Section 3, we will produce rational points on the curves $C_{r^2 b^2 a^{\ell-1}}$. To show that these rational points are not (usually) torsion points, we use the following lemma.

Lemma 2.6. *Let $n \in F^\times$. There are finitely many $t \in F^\times / F^{\times \ell}$ such that $J_{nt^2}(F)_{\mathrm{tors}} \neq J_{nt^2}[\phi](F)$.*

Proof. A version of this lemma holds for the twists of any fixed abelian variety, but the proof in this case is simplified by observing that the Jacobians J_{nt^2} have complex multiplication, hence have everywhere potentially good reduction [ST68, §5]. It follows that there is a uniform upper bound (depending only on ℓ and F) on the order $\# J_{nt^2}(F)_{\mathrm{tors}}$ of the torsion subgroup. Indeed, if $\mathfrak{p}$ is a place of F above a rational prime p, then we may pass to a totally ramified extension of $F_\mathfrak{p}$ over which J_{nt^2} attains good reduction [ST68, p. 498]. We then use the Weil bound over $\mathcal{O}_F/\mathfrak{p}$ to bound the prime-to-p part of $J_{nt^2}(F)_{\mathrm{tors}}$. Applying this to two different primes p gives a bound on $\# J_{nt^2}(F)_{\mathrm{tors}}$. Thus, we may choose an integer N which is a multiple of $\# J_{nt^2}(F)_{\mathrm{tors}}$, for all $t \in F^\times$. Let $\chi_t \colon \mathrm{Gal}(\overline{F}/F) \to \mu_\ell$ be the character $\sigma \mapsto (\sqrt[\ell]{t^2})^\sigma / \sqrt[\ell]{t^2}$, so that there is an isomorphism of $\mathbb{Z}[\zeta][\mathrm{Gal}(\overline{F}/F)]$-modules $J_{nt^2}[N] \simeq J_n[N] \otimes \chi_t^{-1}$. We see that if $J_{nt^2}[N](F)$ contains a point which is not killed by $1 - \zeta$, then the character χ_t is a subrepresentation of $J_n[N]$. This shows that there are only finitely many $t \in F^\times / F^{\times \ell}$ such that $J_{nt^2}(F)_{\mathrm{tors}} \neq J_{nt^2}[\phi](F)$. □

Over $\overline{\mathbb{Q}}$, the curves C_n are μ_ℓ-quotients of the ℓ-th Fermat curve $x^\ell + y^\ell = z^\ell$. We use a twisted version of this covering to produce rational points on $C_{r^2 b^2 a^{\ell-1}}$.

Proposition 2.7. *For all but finitely many $t_{a,b} \in X$, the Jacobian $J_{r^2 a^{\ell-1} b^2}$ has positive rank.*

Proof. For all but finitely many $t_{a,b} \in X$, we have $J_{r^2 a^{\ell-1} b^2}(F)_{\mathrm{tors}} = J_{r^2 a^{\ell-1} b^2}[\phi]$, by Lemma 2.6. Suppose (a, b) is such a pair. Let $\widetilde{C} \colon a x^\ell + 2rby^\ell = z^\ell$ be the twisted Fermat curve and consider the cover $\pi \colon \widetilde{C} \to C_{r^2 a^{\ell-1} b^2}$ given on the affine patch where $z = 1$ by

$$\pi(x, y) = (axy^{-1}, a^{\frac{\ell-1}{2}}(y^{-\ell} - rb)).$$

Since $1 = a + 2rb$, the point $P = (a, a^{\frac{\ell-1}{2}}(1 - rb)) = \pi(1, 1)$ lies in $C_{r^2a^{\ell-1}b^2}(F)$. Since $a \neq 0$, this is not a torsion point, and therefore $J_{r^2a^{\ell-1}b^2}$ has positive rank. □

3 Proof of Proposition 2.5

In this section, we give a proof of Proposition 2.5. The argument is standard, but for convenience in citing the literature, we prove a much stronger result.

Proposition 3.1. *Let F be a totally complex number field. Let $I \subseteq \mathcal{O}_F$ be an ideal. Let $C \in \mathbb{Z}^+$ be prime to I. Let $\beta \in 2\mathcal{O}_F$ be nonzero. Let $u_1, u_2, u_3 \in (\mathcal{O}_F/(C))^\times$ be such that $u_1 + \beta u_2 \equiv u_3 \pmod{C}$. Then there exist infinitely many triples $(p_1, p_2, p_3) \pmod{\mathcal{O}_F^\times}$ such that:*

- *$p_i \in I$ with $\mathrm{Nm}(p_i)/\mathrm{Nm}(I)$ prime;*
- *$p_1 + \beta p_2 = p_3$; and*
- *$p_i \equiv u_i \pmod{C}$.*

Proof. This is a standard modification of Vinogradov's 1937 circle method argument solving ternary Goldbach for sufficiently large integers [Vin04], which was subsequently applied to three-term homogeneous linear equations in the primes by van der Corput [vdC39]. The generalization of the method to number fields is due to Mitsui [Mit60].

We briefly sketch the argument here. One first reduces to needing to estimate the following sum of trigonometric integrals, which counts the number of solutions to $p_1 + \beta p_2 = p_3$ of bounded height:

$$\frac{1}{\left(\mathrm{Nm}_{F/\mathbb{Q}}\, C\right)^3} \sum_{\alpha_1,\alpha_2,\alpha_3 \in \mathcal{O}_F/(C)} e\left(-\frac{\mathrm{tr}_{F/\mathbb{Q}}\left(\alpha_1 u_1 + \alpha_2 u_2 + \alpha_3 u_3\right)}{C}\right) \int_{\xi \in \left(\mathfrak{d}_{F/\mathbb{Q}} I\right)^{-1} \otimes_{\mathbb{Z}} \mathbb{R}/\mathbb{Z}} d\xi\, S_N\left(\xi + \frac{\alpha_1}{C}\right) S_N\left(\beta\xi + \frac{\alpha_2}{C}\right) S_N\left(-\xi + \frac{\alpha_3}{C}\right),$$

where

$$S_N(z) := \sum_{p \in I : ||p||_\infty \leq N} \Lambda_F\left((p)I^{-1}\right) e\left(\mathrm{tr}_{F/\mathbb{Q}}\left(zp\right)\right),$$

and $\Lambda_F := \mu_F * \log$ is the von Mangoldt function of $F/\mathbb{Q}$, and $||x||_\infty := \max_{v|\infty} |x|_v$.

This may be broken up into major and minor arcs in the standard way (with the same height cutoff as in Vinogradov, up to implicit constants), as in [Mit60]. To treat the integral over the major arcs and compute the singular series, we apply Mitsui's number field generalization [Mit56] of the Siegel-Walfisz theorem. For the integral over the minor arcs, we use the Vaughan identity and repeated applications of Cauchy-Schwarz (both for the integral of the remaining two-variable exponential sum over the minor arcs as well as for the Type II sum arising from Vaughan), as in [Mit60]. The additive character modulo C serves to translate the dual vector and thus only affects implicit constants, e.g., in the geometric series estimate on the minor arcs. The finite part of the singular series is (ignoring small primes)

$$\prod_{\mathfrak{p}} \lim_{n \to \infty} \mathrm{Nm}(\mathfrak{p})(\mathrm{Nm}(\mathfrak{p}) - 1)^{-3} \#\{(p_1, p_2) : p_1, p_2, p_1 + \beta p_2 \in (\mathcal{O}_F/\mathfrak{p}^n)^\times\},$$

which is positive by Hensel lifting and the given hypotheses, yielding the desired result.

The proposition can also be deduced from a recent and far more general result of Kai [Kai23], which generalizes to number fields the Green–Tao–Ziegler theorem on simultaneous prime values of linear forms [GTZ12]. For this, let $W \subset I^2$ be the subgroup of $(x, y) \in I^2$ such that $x \equiv u_1$, $y \equiv u_2$, and $x + \beta y \equiv u_3$ modulo C. Define linear maps $\psi_i \colon W \to I$ by $\psi_1(x, y) = x$, $\psi_2(x, y) = y$, and $\psi_3(x, y) = x + \beta y$. By [Kai23, Theorem 13.1], there are infinitely many pairs $(p_1, p_2) \in W$ such that the triple $(p_1, p_2, p_1 + \beta p_2)$ satisfies the three conditions of the proposition. □

Proof of Proposition 2.5. Let $\mathfrak{m}$ be the conductor of K/F, so that $\mathfrak{m}$ is divisible by a prime $\mathfrak{p}$ if and only if $\mathfrak{p}$ ramifies in K/F. The extension K/F corresponds via class field theory to a surjection $\psi \colon \mathrm{Cl}_F(\mathfrak{m}) \to \mathbb{Z}/2\mathbb{Z}$ from the ray class group $\mathrm{Cl}_F(\mathfrak{m})$ of conductor $\mathfrak{m}$. A prime $\mathfrak{p} \nmid \mathrm{Disc}(K/F)$ splits in K if and only if $[\mathfrak{p}] \in \ker(\psi)$.

First suppose that $\mathfrak{m} = 1$, so that K/F is everywhere unramified. Let I be a prime ideal (coprime to S and $r\mathfrak{m}$) such that $[I] \notin \ker(\psi)$. We say that $p \in I$ is an I-prime if $\mathrm{Nm}(p)/\mathrm{Nm}(I)$ is prime. Note that any I-prime p is an S_{inert}-unit, and in particular a Σ-unit. Let γ be any element of $\mathcal{O}_F$ such that $\gamma \in \mathfrak{p}$ if and only if $\mathfrak{p} \in S$. We will apply Proposition 3.1 to the element $\beta = 2r\gamma^{n\ell}$ (for some large integer n to be chosen below as needed) and the ideal I. This gives us I-primes p_1, p_2, p_3 such that $p_1 + 2r\gamma^{n\ell} p_2 = p_3$. We may and will assume that $p_2 \equiv p_3 \pmod{\mathfrak{p}^n}$, for all $\mathfrak{p} \in S$. Now take $a = p_1/p_3$ and $b = \gamma^{n\ell} p_2/p_3$. These are Σ-units and they satisfy $a + 2rb = 1$ by construction. It remains to check that

$$a^{\frac{\ell-1}{2}} b = (1 - 2rb)^{\frac{\ell-1}{2}} \gamma^{n\ell} p_2/p_3$$

lies in $F_{\mathfrak{p}}^{\times \ell}$ for all $\mathfrak{p} \in S$. Since we have chosen n large, the element $1 - 2rb$ is $\mathfrak{p}$-adically close to 1 and hence is an ℓ-th power. Similarly, since n is large and $p_2/p_3 \equiv 1 \pmod{\mathfrak{p}^n}$, the unit p_2/p_3 is an ℓ-th power in $F_{\mathfrak{p}}^{\times}$. Thus $a^{\frac{\ell-1}{2}} b$ is indeed an ℓ-th power in $F_{\mathfrak{p}}^{\times}$, completing the proof in this case.

We now consider the case where $\mathfrak{m} \neq 1$, i.e., where K/F is not a subfield of the Hilbert class field H/F. Applying Chebotarev's Theorem to the compositum HK/F, we see that there exist prime elements p_i of $\mathcal{O}_F$ that are inert in K. Indeed, the restriction of ψ to $\mathrm{Gal}(H_{\mathfrak{m}}/H) \simeq (\mathcal{O}_F/\mathfrak{m})^{\times}/\pi_{\mathfrak{m}}(\mathcal{O}_F^{\times})$ has kernel an index 2 subgroup G_0, and the principal primes p_i that are inert in K/F are those whose images modulo $\mathfrak{m}$ do not lie in G_0. This amounts to a squareclass condition on the primes p_i modulo each prime $\mathfrak{p} \mid \mathfrak{m}$. We now apply Proposition 3.1 to the element $\beta = 2r\gamma^{n\ell}$ and the ideal $I = \mathcal{O}_F$. We define $a = p_1/p_3$ and $b = \gamma^{n\ell} p_2/p_3$ and assume that $p_2 \equiv p_3 \pmod{\mathfrak{p}^n}$ for all $\mathfrak{p} \in S$. Additionally, we prescribe the squareclasses of the p_i modulo each prime dividing $\mathfrak{m}$ so that the p_i are inert in K/F. Since K/F is unramified at primes above ℓ, the sets S and $\{\mathfrak{p} \colon \mathfrak{p} \mid \mathfrak{m}\}$ are disjoint, so the new congruence conditions will not contradict the previous ones. We need only check that the equation

$$t_1 x^2 + 2r\gamma^{n\ell} t_2 y^2 = t_3 z^2$$

has a solution modulo $\mathfrak{m}$ for some choice of units t_1, t_2, t_3 modulo $\mathfrak{m}$. Since we are free to assume $t_1 = t_3$, there is no local obstruction at 2-adic primes $\mathfrak{p} \mid \mathfrak{m}$. For other primes $\mathfrak{p} \mid \mathfrak{m}$, the equation defines a smooth conic modulo $\mathfrak{p}$ and hence is unobstructed as well.

As for infinitude, for each triple (p_1, p_2, p_3) produced by the above construction, the ideal

$$\mathfrak{t}_{p_1,p_2,p_3} := \left(p_1^{\frac{\ell-1}{2}} \; p_2 \; p_3^{\frac{\ell-1}{2}} \right)$$

has large prime factors occurring with multiplicity strictly smaller than ℓ, and moreover the collection of such ideals produced by said construction has infinite support, else we would be producing

infinitely many solutions to an $\mathcal{S}$-unit equation for a finite set $\mathcal{S}$ of primes, contradicting the theorem of Siegel and Mahler. It follows that the set of ℓ-th power classes of the ideals

$$\left(a^{\frac{\ell-1}{2}}b\right) = \mathfrak{t}_{p_1,p_2,p_3}(\gamma^n p_3^{-1})^\ell$$

is infinite, whence the set of ℓ-th power classes of the elements $a^{\frac{\ell-1}{2}}b$ is infinite as well. □

4 Proof of the main theorem (Theorem 1.1)

In this section, for any quadratic extension K/F of number fields, we construct an abelian variety A/F with the property that $\operatorname{rank} A(F) = \operatorname{rank} A(K) > 0$.

Let ℓ be an odd prime not dividing the discriminant of K. Then K and the ℓ-th cyclotomic field $\mathbb{Q}(\zeta_\ell)$ are linearly disjoint inside a common algebraic closure. By the Weil restriction construction, it is enough to prove the theorem for the quadratic extension $K(\zeta_\ell)/F(\zeta_\ell)$. Hence we may assume that $\zeta_\ell \in F$ and K/F is unramified at primes above ℓ, i.e., we are in the setting of §2.3.

Let $K = F(\sqrt{q})$, and choose r as in Lemma 2.3. Then choose a, b as in Proposition 2.7, so that $\operatorname{rank} J_{r^2a^{\ell-1}b^2}(F) > 0$. Lemmas 2.1 and 2.4 imply that $J_{q^\ell r^2 a^{\ell-1}b^2}(F)$ has rank 0. It follows that

$$\operatorname{rank} J_{r^2a^{\ell-1}b^2}(K) = \operatorname{rank} J_{r^2a^{\ell-1}b^2}(F) + \operatorname{rank} J_{q^\ell r^2 a^{\ell-1}b^2}(F) = \operatorname{rank} J_{r^2a^{\ell-1}b^2}(F) > 0,$$

so that $A := J_{r^2a^{\ell-1}b^2}$ over F is the sought-after abelian variety.

We have proven Theorem 1.1, and therefore Corollary 1.2 also follows.

Acknowledgments

We thank Tim Dokchitser, Vladimir Dokchitser, Peter Koymans, Jef Laga, Robert Lemke Oliver, Barry Mazur, Adam Morgan, Carlo Pagano, Hector Pasten, Bjorn Poonen, Arul Shankar, and Alexandra Shlapentokh for helpful conversations and comments. LA was supported by NSF DMS-2002109 and the Society of Fellows. MB was partially supported by a Simons Investigator Grant and NSF DMS-1001828. WH was partially supported by NSF DMS-2309115, the Minerva Research Foundation, and a grant from the Institute for Advanced Study. AS was partially funded by the European Research Council (ERC, CurveArithmetic, 101078157), as well as the Ambrose Monell Foundation while at the Institute of Advanced Study.

References

[CPZ05] Gunther Cornelissen, Thanases Pheidas, and Karim Zahidi, *Division-ample sets and the Diophantine problem for rings of integers*, J. Théor. Nombres Bordeaux **17** (2005), no. 3, 727–735. MR 2212121

[DPR61] Martin Davis, Hilary Putnam, and Julia Robinson, *The decision problem for exponential diophantine equations*, Ann. of Math. (2) **74** (1961), 425–436. MR 133227

[GTZ12] Ben Green, Terence Tao, and Tamar Ziegler, *An inverse theorem for the Gowers $U^{s+1}[N]$-norm*, Ann. of Math. (2) **176** (2012), no. 2, 1231–1372. MR 2950773

[Hil02] David Hilbert, *Mathematical problems*, Bull. Amer. Math. Soc. **8** (1902), no. 10, 437–479. MR 1557926

[Kai23] Wataru Kai, *Linear patterns of prime elements in number fields*, Preprint, available at https://arxiv.org/abs/2306.16983, 2023+.

[KP24] Peter Koymans and Carlo Pagano, *Hilbert's tenth problem via additive combinatorics*, Arxiv preprint, available at https://arxiv.org/abs/2412.01768, 2024+.

[Mc70] Ju.Ṽ. Matijasevič, *The Diophantineness of enumerable sets*, Dokl. Akad. Nauk SSSR **191** (1970), 279–282. MR 258744

[Mit56] Takayoshi Mitsui, *Generalized prime number theorem*, Jpn. J. Math. **26** (1956), 1–42. MR 92814

[Mit60] ———, *On the Goldbach problem in an algebraic number field. I, II*, J. Math. Soc. Japan **12** (1960), 290–324, 325–372. MR 136590

[MR10] B. Mazur and K. Rubin, *Ranks of twists of elliptic curves and Hilbert's tenth problem*, Invent. Math. **181** (2010), no. 3, 541–575. MR 2660452

[MRS24] Barry Mazur, Karl Rubin, and Alexandra Shlapentokh, *Existential definability and diophantine stability*, J. Number Theory **254** (2024), 1–64. MR 4633727

[Poo02] Bjorn Poonen, *Using elliptic curves of rank one towards the undecidability of Hilbert's tenth problem over rings of algebraic integers*, Algorithmic number theory (Sydney, 2002), Lecture Notes in Comput. Sci., vol. 2369, Springer, Berlin, 2002, pp. 33–42. MR 2041072

[Shl08] Alexandra Shlapentokh, *Elliptic curves retaining their rank in finite extensions and Hilbert's tenth problem for rings of algebraic numbers*, Trans. Amer. Math. Soc. **360** (2008), no. 7, 3541–3555. MR 2386235

[ST68] Jean-Pierre Serre and John Tate, *Good reduction of abelian varieties*, Ann. of Math. (2) **88** (1968), 492–517. MR 236190

[SW23] Ari Shnidman and Ariel Weiss, *Rank growth of elliptic curves over N-th root extensions*, Trans. Amer. Math. Soc. Ser. B **10** (2023), 482–506. MR 4575766

[vdC39] J. G. van der Corput, *Über Summen von Primzahlen und Primzahlquadraten*, Math. Ann. **116** (1939), no. 1, 1–50. MR 1513216

[Vin04] I. M. Vinogradov, *The method of trigonometrical sums in the theory of numbers*, Dover Publications, Inc., Mineola, NY, 2004, Translated from the Russian, revised and annotated by K. F. Roth and Anne Davenport, Reprint of the 1954 translation. MR 2104806

[Yu16] Myungjun Yu, *Selmer ranks of twists of hyperelliptic curves and superelliptic curves*, J. Number Theory **160** (2016), 148–185. MR 3425203