REVISITING THE LIND–REICHARDT COUNTEREXAMPLE TO HASSE'S LOCAL-GLOBAL PRINCIPLE

Abstract. We discuss what is widely believed to be the first published counterexample to the Hasse principle, presented by Hans Reichardt in 1942: The equation $X^4 - 17Y^4 = 2Z^2$ has no nonzero solution in rational numbers X, Y, Z, but has a nonzero solution over $\mathbb{R}$ and over every $\mathbb{Q}_p$. We demonstrate that Reichardt's example can be presented in a completely elementary way. Both local solvability and global unsolvability can be established using tools no deeper than quadratic reciprocity. For global solvability, this has long been known, but our simple and short proof of local solvability appears to be new. The above counterexample is usually attributed to Lind as well as Reichardt. We discuss how this claim, while correct, is *not correct enough* due to the presence of a third individual who made contributions to this problem.

1. Introduction

In number theory, the term *local-global principle* refers to an expression of mathematical optimism. It predicts that properties of interest hold in the field of rational numbers $\mathbb{Q}$ (hold *globally*) precisely when they hold in $\mathbb{R}$ and in all fields $\mathbb{Q}_p$, where p ranges over the set of prime numbers (hold *everywhere locally*).[1] Here $\mathbb{Q}_p$ is the field of *p-adic numbers*, which for each prime p is constructed as a completion of $\mathbb{Q}$ with respect to a p-adic metric, analogously to how the real numbers $\mathbb{R}$ are constructed as the completion of $\mathbb{Q}$ with respect to the familiar Archimedean metric. For the elementary theory of $\mathbb{Q}_p$ (much more than needed here), readers are referred to Gouvêa's highly engaging textbook [Gou20].

The fields $\mathbb{Q}_p$ were originally introduced by Kurt Hensel at the end of the 19th century. Each element of $\mathbb{Q}_p$ captures information modulo p^n for all $n \geq 1$. This encoding often allows statements about congruences to be translated into statements about equations in $\mathbb{Q}_p$. As one application of this dictionary, if $f(x)$ is a monic polynomial with integer coefficients, then the equation $f(x) = 0$ is solvable in every $\mathbb{Q}_p$ if and only if the corresponding congruence is solvable modulo m for every positive integer m.

The idea of the local-global principle is due to Hensel (see [Has62]), but its first concrete instantiations were formulated and proved by Hensel's student Helmut Hasse, and it has become customary to use the names *local-global principle* and *Hasse principle* interchangeably.

Applied to polynomial equations, the Hasse principle forecasts that a polynomial with $\mathbb{Q}$-coefficients (or a system of such) has a nontrivial zero over $\mathbb{Q}$ (simultaneous zero,

[1] The local-global principle can be — and usually is — formulated much more generally, for instance for all number fields or even all global fields. We stick to $\mathbb{Q}$ for simplicity.

in the case of a system) precisely when there is zero over $\mathbb{R}$ and a zero over each $\mathbb{Q}_p$. Taking advantage of modern theory, it is usually straightforward (and always algorithmically decidable) to determine whether there are zeros everywhere locally. By contrast, deciding for a given system of polynomials whether there is a zero over $\mathbb{Q}$ often requires extraordinary ingenuity, and the general problem may well be algorithmically undecidable. Thus, when the Hasse principle holds, we have an easy way of answering a hard-seeming question.

The Hasse principle gets its name from the groundbreaking work of Hasse in the early 1920s [Has23], showing that the principle holds for every homogeneous quadratic polynomial (quadratic form). Nowadays we know many counterexamples to this polynomial version of the local-global principle. For instance, the Hasse principle is generally not valid for cubic forms. Yet rather than doom the local-global principle to the dustbin, these failures of the Hasse principle have proved every bit as valuable as its successes in terms of generating valuable mathematics (see the survey [SD04]). As a consequence, the local-global principle remains a central object of study in arithmetic geometry.

In this paper, we revisit what is widely believed to be the first published counterexample to the (polynomial) Hasse principle, presented by Hans Reichardt in 1942: *The equation*

$$X^4 - 17Y^4 = 2Z^2 \tag{1}$$

has no nonzero solution in rational numbers X, Y, Z, but has a nonzero solution over $\mathbb{R}$ and over every $\mathbb{Q}_p$ [Rei42].

Our aim is two-fold:

(a) We demonstrate that Reichardt's example can be presented in a completely elementary way. Both the local solvability of (1), and its global unsolvability, can be established using tools no deeper than quadratic reciprocity. For global solvability, this has long been known, but our simple and short proof of local solvability appears to be new.

(b) The counterexample (1) is usually attributed to Lind (1940, [Lin40]), as well as Reichardt. We discuss how this claim, while correct, is *not correct enough*.

Since it does not introduce any serious difficulties and will be helpful for our historical survey, we will focus our discussion of local and global solvability around a generalization of (1). Let ℓ be a prime, $\ell \equiv 1 \pmod 8$, for which 2 is not a 4^{th} power modulo ℓ. For example, $\ell = 17$ is such a prime. We show in §2 that

$$X^4 - \ell Y^4 = 2Z^2 \tag{2}$$

has no global solution and in §3 that it has local solutions everywhere. One can show using the Chebotarev density theorem that 1/8 of all primes ℓ meet the imposed conditions; thus the equations (2) constitute an infinite family of counterexamples to the Hasse principle.

There are much easier counterexamples to the Hasse principle. For example, let a, b be nonzero square-free integers, satisfying $\gcd(a, b) = 1$. Assume that at least one of a, b, and ab is congruent to 1 mod 8, and that a is a square mod $|b|$ and b is a square mod $|a|$. Finally, assume that none of a, b, and ab is a square in $\mathbb{Z}$. Then the equation $(x^2 - a)(x^2 - b)(x^2 - ab) = 0$ has a solution in $\mathbb{Q}_p$ for every p and also a solution in $\mathbb{R}$, but has no solution in $\mathbb{Q}$. The lack of a global solution is clear. There is a solution in $\mathbb{R}$ because at least one of a, b, ab is positive. The existence of everywhere local solutions is straightforward to verify using Hensel's Lemma (Lemma 1 below) and the other ideas in this paper. One suspects such counterexamples to the Hasse principle must have been noticed early on; however, we are not aware of an example in this family being explicitly mentioned until a 1942 paper of Skolem (see p. 4 of [Sko42]) where the case $a = 2$ and $b = -7$ appears.

While the simple examples in the last paragraph suffice to refute the polynomial Hasse principle, they are uninteresting geometrically: Their defining polynomials factor and the corresponding zero loci are finite. The failures of the form (2) are of greater significance. Specifically, each counterexample of the form (2) yields a nontrivial (order two) element in the Tate–Shafarevich group of a certain elliptic curve (given in Weierstrass form by $y^2 = x^3 - \ell x$; this is the Jacobian of the genus one curve over $\mathbb{Q}$ that (2) defines in weighted projective space). More details can be found in [AL11, Appendix B]. The Tate–Shafarevich group is a central object of study in modern arithmetic geometry.

We will use the following notations in this paper. For a prime p, $\mathbb{F}_p$ denotes $\mathbb{Z}/p\mathbb{Z}$, the field with p elements. Thus equality in $\mathbb{F}_p$ is the same as congruence modulo p. We let $\mathbb{F}_p^\times$ denote the group of nonzero elements of $\mathbb{F}_p$, and we let $\mathbb{F}_p^2$ and $(\mathbb{F}_p^\times)^2$ denote the set of squares and the set of nonzero squares, respectively, in $\mathbb{F}_p$.

2. Equation (2) has no global solution

The argument of this section is not new (compare with [Sch07, Satz 3.5.9, pp. 46–47] or [Cas66, Appendix A, p. 284]), but is included for completeness. We will need to use the following consequence of Gauss' Quadratic Reciprocity Law. If ℓ is a prime congruent to 1 modulo 4, p is any odd prime, and ℓ is a nonzero square modulo p, then p is a nonzero square modulo ℓ.

Assume (X, Y, Z) is a nonzero rational solution to (2). Scaling X, Y, and Z by factors D, D, and D^2, respectively, for an appropriately chosen D, we can assume that X, Y, and Z are integers.

If there is a prime p that divides X and Y, then $p^4 \mid X^4 - \ell Y^4 = 2Z^2$, forcing p^2 to divide Z. In that case, $(X/p, Y/p, Z/p^2)$ is also an integer solution to (2), and the sum of the absolute values of the components has decreased in size. Successively removing prime divisors of $\gcd(X, Y)$ in this way, we eventually reach an integer solution where $\gcd(X, Y) = 1$. The form of (2) then guarantees that $\gcd(X, Z) = 1$ and $\gcd(Y, Z) = 1$.

Since $\sqrt[4]{\ell} \notin \mathbb{Q}$ and $(X, Y, Z) \neq (0, 0, 0)$, we cannot have $Z = 0$. Replacing Z with $-Z$ if necessary, we can assume that $Z > 0$.

Let p be any odd prime dividing Z. Then $p \nmid XY$. Reducing (2) modulo p, we find that $\ell = (X/Y)^4$ in $\mathbb{F}_p$. In particular, ℓ is a nonzero square modulo p, so that from Gauss's law of quadratic reciprocity, p is a nonzero square modulo ℓ. We assumed that $\ell \equiv 1 \pmod 8$, so 2 is also a nonzero square modulo ℓ. (We give a simple proof below of this in Lemma 3 (ii).) Since $Z > 0$ and every prime factor of Z is a nonzero square modulo ℓ, it follows that Z is a nonzero square modulo ℓ.

Choose an integer W, not divisible by ℓ, with $Z \equiv W^2 \pmod \ell$. Then

$$X^4 \equiv X^4 - \ell Y^4 = 2Z^2 \equiv 2W^4 \bmod \ell,$$

so that $(X/W)^4 \equiv 2 \bmod \ell$. But 2 is not a 4^{th} power modulo ℓ. Contradiction!

3. Equation (2) is everywhere locally solvable

For a polynomial f with integer coefficients, Hensel's Lemma provides a way to extend certain solutions of the congruence $f(x) \equiv 0 \bmod p$ to solutions of $f(x) = 0$ in $\mathbb{Q}_p$. We now give a common form of Hensel's lemma (appearing, for example, as [Ser73, Theorem 1, p. 14]).

Lemma 1. *Let $f \in \mathbb{Z}[X]$, let f' denote the derivative of f, let p be a prime number, and let $e \in \mathbb{Z}$ with $e \geq 0$. If there is a $c \in \mathbb{Z}$ with $f(c) \equiv 0 \bmod p^{2e+1}$ and $f'(c) \not\equiv 0 \bmod p^{e+1}$, then there is an $\alpha \in \mathbb{Q}_p$ for which $f(\alpha) = 0$.*

For our purposes, the following two consequences of Hensel's lemma suffice.

Lemma 2.

(i) *Suppose that p is an odd prime and $a \in \mathbb{Z}$ is not divisible by p. If a is a square modulo p, then a is a square in $\mathbb{Q}_p$. The same statement holds if "square" is replaced by "4^{th} power."*

(ii) *Suppose that $a \in \mathbb{Z}$. If $a \equiv 1 \bmod 8$, then a is a square in $\mathbb{Q}_2$. If $a \equiv 1 \bmod 16$, then a is a 4^{th} power in $\mathbb{Q}_2$.*

Proof. (i) Let $f(x) = x^n - a$ where $n = 2$ or 4 (or any integer not divisible by p). Since a is an n^{th} power modulo p, there exists $c \in \mathbb{Z}$ satisfying $f(c) \equiv 0 \bmod p$. Since $f'(c) = nc^{n-1} \not\equiv 0 \bmod p$, Hensel's lemma (applied with $e = 0$) implies that a is an n^{th} power in $\mathbb{Q}_p$.

(ii) Suppose that $a \equiv 1 \bmod 8$, and let $f(x) = x^2 - a$ and let $c = 1$. Then $f(c) \equiv 0 \bmod 2^3$ and $f'(c) = 2c \not\equiv 0 \bmod 4$. Hensel's lemma (applied with $e = 1$) implies that a is a square in $\mathbb{Q}_2$.

Suppose that $a \equiv 1 \bmod 16$, and let $f(x) = x^4 - a$. If $a \equiv 1 \bmod 32$, let $c = 1$, and if $a \equiv 17 \bmod 32$, let $c = 3$. Then $f(c) \equiv 0 \bmod 2^5$ and $f'(c) = 4c^3 \not\equiv 0 \bmod 2^3$. Hensel's lemma (applied with $e = 2$) implies that a is a 4^{th} power in $\mathbb{Q}_2$. □

Lemma 3. *Let p be an odd prime.*

(i) $-1 \in \mathbb{F}_p^2$ *if and only if* $p \equiv 1 \bmod 4$.

(ii) $-1 \in \mathbb{F}_p^4$ *if and only if* $p \equiv 1 \bmod 8$. *For such p,* $2 \in \mathbb{F}_p^2$.

(iii) *The quotient group* $\mathbb{F}_p^\times/(\mathbb{F}_p^\times)^2$ *has order* 2.

(iv) *The quotient group* $(\mathbb{F}_p^\times)^2/(\mathbb{F}_p^\times)^4$ *has order* 2 *if* $p \equiv 1 \bmod 4$, *and has order* 1 *if* $p \equiv 3 \bmod 4$.

Proof. We use repeatedly that $\mathbb{F}_p^\times$ is a cyclic group of order $p-1$ (see for instance [Ser73, p. 4]). Let a be a generator, so that $\mathbb{F}_p^\times = \langle a \rangle$.

(i) If $p \equiv 1 \bmod 4$, let $b = a^{\frac{p-1}{4}}$. Then $b^4 = 1$ and $b^2 \neq 1$, so $b^2 = -1$, and -1 is a square. Conversely, if there exists $b \in \mathbb{F}_p$ with $b^2 = -1$, then b has order 4 in $\mathbb{F}_p^\times$, which implies that $4 \mid p-1$.

(ii) If $p \equiv 1 \bmod 8$, let $c = a^{\frac{p-1}{8}}$. Then c has order 8 and $c^4 = -1$ is a fourth power in $\mathbb{F}_p^\times$. Conversely, if there exists $c \in \mathbb{F}_p$ with $c^4 = -1$, then c has order 8 in $\mathbb{F}_p^\times$, which implies that $8 \mid p-1$.

For the second statement, if $c^4 = -1$, then $(c + c^{-1})^2 = 2 + c^{-2}(c^4 + 1) = 2$.

(iii) We have $\mathbb{F}_p^\times = \langle a \rangle$, $(\mathbb{F}_p^\times)^2 = \langle a^2 \rangle$, and $(\mathbb{F}_p^\times)^4 = \langle a^4 \rangle$. Since $p-1$ is even, it follows that $|(\mathbb{F}_p^\times)^2| = (p-1)/2$.

(iv) If $p \equiv 1 \bmod 4$, then a^4 has order $(p-1)/4$, so $(\mathbb{F}_p^\times)^2/(\mathbb{F}_p^\times)^4$ has order 2. If $p \equiv 3 \bmod 4$, then $(\mathbb{F}_p^\times)^2 = (\mathbb{F}_p^\times)^4$, because

$$a^2 = a^2 a^{p-1} = \left(a^{(p+1)/4}\right)^4 \in (\mathbb{F}_p^\times)^4.$$ □

Proof that (2) *is everywhere locally solvable.* The following five points satisfy the equation $X^4 - \ell Y^4 = 2Z^2$:

$$P_1 = (\ell^{1/4}, 1, 0), \qquad P_2 = ((\ell+8)^{1/4}, 1, 2), \qquad P_3 = (\sqrt{2}, 0, \sqrt{2}),$$

$$P_4 = ((-\ell)^{1/4}, 1, ((-\ell)^{1/4})^2), \qquad P_5 = (0, 2, 2\sqrt{-2\ell}).$$

Each of P_1, P_2, and P_3 is an $\mathbb{R}$-solution to (2).

Suppose that $p = 2$. Since $\ell \equiv 1 \pmod 8$, either ℓ or $\ell + 8$ is congruent to 1 modulo 16, so one of $\ell^{1/4}$ or $(\ell+8)^{1/4}$ exists in $\mathbb{Q}_2$ by Lemma 2 (ii). Then either P_1 or P_2 is a $\mathbb{Q}_2$-solution to (2).

Since $\ell \equiv 1 \bmod 8$, Lemma 3 (ii) implies that $2 \in \mathbb{F}_\ell^2$. Lemma 2 (i) then implies that $\sqrt{2}$ exists in $\mathbb{Q}_\ell$ so that P_3 is a $\mathbb{Q}_\ell$-solution.

It remains to find a $\mathbb{Q}_p$-solution for every odd prime p with $p \neq \ell$.

If $\ell \in \mathbb{F}_p^4$, then Lemma 2 (i) implies that $\ell^{1/4}$ exists in $\mathbb{Q}_p$ and P_1 is a $\mathbb{Q}_p$-solution to (2). Similarly, if $-\ell \in \mathbb{F}_p^4$, or $2 \in \mathbb{F}_p^2$, or $-2\ell \in \mathbb{F}_p^2$, then P_4, or P_3, or P_5 provides a $\mathbb{Q}_p$-solution to (2).

If those cases all fail, then p is an odd prime with $p \neq \ell$ and the following holds:

$$\ell \text{ and } -\ell \text{ are not in } \mathbb{F}_p^4, \text{ and } 2 \text{ and } -2\ell \text{ are not in } \mathbb{F}_p^2.$$

We will show that these conditions lead to a contradiction.

Lemma 3 (iii) implies that $-\ell = 2^{-1} \cdot (-2\ell) \in \mathbb{F}_p^2$. If $p \equiv 3 \bmod 4$, then Lemma 3 (iv) implies that $-\ell \in \mathbb{F}_p^2 = \mathbb{F}_p^4$, contrary to hypothesis. Therefore $p \equiv 1 \bmod 4$ and Lemma 3 (i) shows that $-1 \in \mathbb{F}_p^2$. Then $\ell = (-1)(-\ell) \in \mathbb{F}_p^2$.

Since ℓ and $-\ell$ are in $\mathbb{F}_p^2$, but not in $\mathbb{F}_p^4$, and $(\mathbb{F}_p^\times)^2/(\mathbb{F}_p^\times)^4$ has order 2 by Lemma 3 (iv), it follows that $-1 = \ell^{-1}(-\ell) \in \mathbb{F}_p^4$. But Lemma 3 (ii) then implies that $2 \in \mathbb{F}_p^2$, contrary to hypothesis. □

Remarks. Reichardt proved the local solvability of (1) by appealing to a 1931 theorem of F. K. Schmidt, Satz 20 of [Sch31]. As long as $p \neq 2$ or 17, we can view (1) as defining a smooth, genus 1 curve over $\mathbb{F}_p$. The existence of a nonzero $\mathbb{F}_p$-solution to (1) follows from the existence of a degree one prime divisor in the associated function field. That we always have such a divisor is a straightforward corollary of Schmidt's result. From an $\mathbb{F}_p$-solution, Hensel's Lemma produces a $\mathbb{Q}_p$-solution. The primes $p = 2$ and $p = 17$ must be treated separately, but (as seen above) this is easy. This proof can be adapted to treat a wide class of curves including (2).

In [AL11], Aitken and Lemmermeyer propose a different method to prove the local solvability of equations $aX^4 + bX^2Y^2 + cY^4 = dZ^2$. Their idea is to leverage the classical parametrization of points on the underlying conic $aU^2 + bUV + cV^2 = dZ^2$. This elegant proof, although not as short as the one offered above, has the advantage of applying to a wider class of curves than (2).

Finally, while our approach to the local solvability of (2) seems to be new, arguments in the same spirit have appeared before. For example, Coray [Cor20, Exercises 9.1–9.3, p. 139; solutions on p. 171] and Conrad [Con] both prove the local solvability of $3x^3 + 4y^3 + 5z^3 = 0$ (a counterexample to the Hasse principle due to Selmer) by reducing appropriately chosen points.

4. Lind? Reichardt? Billing? Oh my!

Who gave us the counterexample (1)? There is no mystery as to why Reichardt has his name attached to (1). This equation appears on the first page of the paper [Rei42], and is explicitly trumpeted as a counterexample to the local-global principle. The title

of Reichardt's paper translates to "A Diophantine equation solvable everywhere in the small but unsolvable in the large"; here "in the small" and "in the large" are quaint terms for "local" and "global".

One often reads that Carl-Erik Lind constructed the counterexample (1) around the same time as Reichardt. Chapter VI of Lind's 1940 PhD thesis [Lin40] is a detailed study of when an equation of the form $aX^4 + bX^2Y^2 + cY^4 = dZ^2$ admits a nonzero rational (equivalently, integer) solution. The specific equation (1) is never mentioned, but the unsolvability of the equations (2) — and in particular of the equation (1) — is a special case of Satz 4 (I,1) on p. 64 of [Lin40]. So Lind should surely be credited with proving that (1) has no nonzero $\mathbb{Q}$-solution. In fact, the proof of global unsolvability we presented in §2 is a simplified version of Lind's. Reichardt's argument for the unsolvability of (1) was significantly more involved, based on a determination of the $\mathbb{Q}(\sqrt{2})$-solutions to $X^4 + 17Y^4 = Z^2$.

It is less clear that Lind should be credited with (1) *as a counterexample to the Hasse principle*. Lind is not concerned in [Lin40] with the Hasse principle, and one looks in vain for any mention of p-adic numbers or local solvability. For a modern arithmetic geometer, local solvability is essentially automatic (as a result of Schmidt's theorem or the later, more difficult "Weil bound" [Wei48]), and it is obvious when reading [Lin40] that Lind is presenting a counterexample to the Hasse principle. What is doubtful is whether Lind realized that he was doing so! Reichardt was certainly better positioned to be thinking about matters connected with the local-global principle, being a student of Hasse at Marburg.

If we accept that both Lind and Reichardt gave us (1), who was first? According to the cover page of Lind's thesis, his defense was scheduled for May 22, 1940. Reichardt's paper was received by Crelle [2] on September 16, 1940. So it would seem Lind beat Reichardt to this particular mountaintop, if only by a few months.

However, there is a twist in the story that appears to have gone unreported! As pointed out to us by Dino Lorenzini, both Lind and Reichardt were anticipated by Gunnar Billing. Billing, like Lind, was a student of Trygve Nagell in Uppsala, but he preceded Lind. As indicated on the cover of Billing's thesis [Bil38], Billing's results were reported to the Royal Society of the Sciences in Uppsala already on October 15, 1937.

On p. 109 of [Bil38], it is proved that if $\ell \equiv 1 \pmod 8$ and 2 is not a 4^{th} power mod ℓ, then there are no nonzero rational solutions to the system

$$\begin{aligned} 2Z^2 &= X^2 - \ell Y^2 \\ W^2 &= XY. \end{aligned} \tag{3}$$

Billing's result is equivalent to the unsolvability of (2).

[2] Crelle is a common nickname for the Journal für die reine und angewandte Mathematik. August Leopold Crelle was the founder and first editor of this journal.

Proposition 4. *For each positive integer ℓ, the following are equivalent.*

(i) *There are no nonzero rational solutions to the system*

$$2Z^2 = X^2 - \ell Y^2$$
$$W^2 = XY.$$

(ii) $X^4 - \ell Y^4 = 2Z^2$ *has no nonzero rational solution.*

Proof. Suppose that there is a nonzero rational solution of the system (i). Then there is a solution where X, Y, Z, W are integers with $X, Y > 0$ and $\gcd(X, Y) = 1$. By unique factorization, $X = x^2$ and $Y = y^2$ with $x, y \in \mathbb{Z}$, and we get $x^4 - \ell y^4 = 2Z^2$.

Conversely, suppose that $X^4 - \ell Y^4 = 2Z^2$ has a nonzero rational solution. Then there exist integers $x, y, z \in \mathbb{Z}$, not all zero, such that $x^4 - \ell y^4 = 2z^2$. Let $X = x^2, Y = y^2, Z = z$, and $W = xy$. Then X, Y, Z, W satisfy (i). □

Lind references parts of Billing's thesis multiple times in [Lin40], so he was clearly acquainted with Billing's thesis and some results contained in it. What is less certain, and left open by these references, is whether Lind was aware that his results on (2) also overlap with Billing's work.

In the interest of giving Billing what he is owed, it seems appropriate to conclude this paper with Billing's forgotten proof that (2) has no nonzero global solution. We describe his argument for the unsolvability of (2) in such a way as to avoid explicit mention of the system (3).

Recall that for a prime p and integers m and t, with $t \geq 0$, the notation $p^t \parallel m$ indicates that $p^t \mid m$ while $p^{t+1} \nmid m$.

Lemma 5. *Let U and V be integers, not both 0, and let p be a prime congruent to 5 or 7 modulo 8.*

(i) *If $p \mid U^2 + 2V^2$, then $p \mid \gcd(U, V)$.*

(ii) *If $p^t \parallel \gcd(U, V)$, then $p^{2t} \parallel U^2 + 2V^2$.*

The proof of this lemma requires the elementary result that -2 is a nonzero square modulo a prime p precisely when $p \equiv 1$ or $3 \bmod 8$ (see, e.g. [Ser73, pp. 6–7]).

Proof of Lemma 5. Let p be a prime congruent to 5 or 7 modulo 8 that divides $U^2 + 2V^2$, and suppose that p does not divide $\gcd(U, V)$. Since $U^2 \equiv -2V^2 \pmod{p}$, and $p \nmid \gcd(U, V)$, it must be that $p \nmid V$. Then $(U/V)^2 = -2$ in $\mathbb{F}_p$. But -2 is not a square modulo p as p is neither 1 nor 3 modulo 8. This contradiction completes the proof of (i).

(ii) Let $U' = U/p^t$ and $V' = V/p^t$. Then (i) implies that $p \nmid U'^2 + 2V'^2$. Hence, $p^{2t} \parallel p^{2t}(U'^2 + 2V'^2) = U^2 + 2V^2$. □

The proof of Theorem 6 below requires Fermat's 2-square theorem, which states that if ℓ is a prime with $\ell \equiv 1 \bmod 4$, then ℓ can be written $\ell = u^2 + v^2$ for positive integers u, v where u is even. If $\ell \equiv 1 \bmod 8$, then since $v^2 \equiv 1 \bmod 8$, it follows that $4 \mid u$.

Theorem 6 (Billing)**.** *Let ℓ be a prime, $\ell \equiv 1 \bmod 8$. Write $\ell = u^2 + v^2$ where $u, v \in \mathbb{Z}$ and $4 \mid u$. If $u \equiv 4 \bmod 8$, then there are no nonzero rational solutions to the equation $X^4 - \ell Y^4 = 2Z^2$.*

Readers might reasonably object that this is not the theorem they were promised: The expected condition "2 is not a 4^{th} power mod ℓ" has been replaced by "$u \equiv 4 \pmod 8$". However, as noted on p. 115 of Billing's thesis, Gauss proved that the two requirements on ℓ are equivalent for primes $\ell \equiv 1 \pmod 8$ [Gau27]. (See also Dirichlet's paper [Dir60], and compare with Exercises 26–28 on p. 64 of [IR90].)

Proof. Assume that (X, Y, Z) is a nonzero solution to $X^4 - \ell Y^4 = 2Z^2$. Just as in Section 2, there is a solution with $X, Y, Z \in \mathbb{Z}$ with $\gcd(X, Y) = 1$. Since $X \equiv Y \bmod 2$, it follows that X, Y are both odd. We have

$$2Z^2 = X^4 - \ell Y^4 = X^4 - (u^2 + v^2)Y^4,$$

$$v^2 Y^4 + 2Z^2 = X^4 - u^2 Y^4 = (X^2 + uY^2)(X^2 - uY^2).$$

Furthermore, $X^2 + uY^2 \equiv 5 \bmod 8$ because X, Y are both odd.

This last congruence on $X^2 + uY^2$ implies that there is a prime power $p^t \parallel X^2 + uY^2$ with p^t being 5 or 7 mod 8. Then p is 5 or 7 mod 8 and t is odd.

Claim. $p \nmid X^2 - uY^2$.

Indeed, if $p \mid X^2 - uY^2$, then $p \mid 2X^2$ and $p \mid 2uY^2$. Since p is odd and $\gcd(X, Y) = 1$, it must be that $p \nmid Y$ and $p \mid u$. If $p \mid v$, then $p^2 \mid u^2 + v^2 = \ell$, which is absurd. So $p \nmid v$. Therefore $p \nmid vY^2$ and so $p \nmid \gcd(vY^2, Z)$. Then Lemma 5 (i) implies that

$$p \nmid (vY^2)^2 + 2Z^2 = (X^2 + uY^2)(X^2 - uY^2),$$

a contradiction because $p \mid X^2 + uY^2$. This contradiction proves the Claim.

This Claim and the definition of p^t imply that $p^t \parallel (X^2+uY^2)(X^2-uY^2) = (vY^2)^2+2Z^2$. As t is odd, this contradicts Lemma 5 (ii). □

Remark. In contrast with our earlier proof, Billing's argument uses only the quadratic character of -2, rather than depending on the Quadratic Reciprocity Law.

Acknowledgements

BLINDED FOR REVIEW.

References

[AL11] W. Aitken and F. Lemmermeyer, *Counterexamples to the Hasse principle*, Amer. Math. Monthly **118** (2011), 610–628.

[Bil38] G. Billing, *Beiträge zur arithmetischen Theorie der ebenen kubischen Kurven vom Geschlecht Eins*, University of Uppsala, Uppsala, 1938, doctoral thesis.

[Cas66] J. W. S. Cassels, *Diophantine equations with special reference to elliptic curves*, J. London Math. Soc. **41** (1966), 193–291.

[Con] K. Conrad, *Selmer's example*, online expository paper. URL: `https://kconrad.math.uconn.edu/blurbs/gradnumthy/selmerexample.pdf`. Accessed 11/27/2024.

[Cor20] D. Coray, *Notes on geometry and arithmetic*, Universitext, Springer, Cham, 2020.

[Dir60] P. G. L. Dirichlet, *Über den biquadratischen Charakter der Zahl "Zwei"*, J. Reine Angew. Math. **57** (1860), 187–188, also appears as paper XXIV in: *Werke*, vol. II, Chelsea, New York, 1969, pp. 261-262.

[Gau27] C. F. Gauss, *Theoria residuorum biquadraticorum, commentatio prima*, Comment. Soc. regiae sci. Göttingen **6** (1823–1827), 27–56, also in: *Untersuchungen über höhere Arithmetik*, Chelsea Publishing Co., New York, 1965, pp. 511–533.

[Gou20] F. Q. Gouvêa, *p-adic numbers: An introduction*, third ed., Universitext, Springer, Cham, 2020.

[Has23] H. Hasse, *Über die Darstellbarkeit von Zahlen durch quadratische Formen im Körper der rationalen Zahlen*, J. Reine Angew. Math. **152** (1923), 129–148.

[Has62] ———, *Kurt Hensels entscheidender Anstoss zur Entdeckung des Lokal-Global-Prinzips*, J. Reine Angew. Math. **209** (1962), 3–4.

[IR90] K. Ireland and M. Rosen, *A classical introduction to modern number theory*, second ed., Graduate Texts in Mathematics, vol. 84, Springer-Verlag, New York, 1990.

[Lin40] C.-E. Lind, *Untersuchungen über die rationalen Punkte der ebenen kubischen Kurven vom Geschlecht Eins*, University of Uppsala, Uppsala, 1940, doctoral thesis.

[Rei42] H. Reichardt, *Einige im Kleinen überall lösbare, im Grossen unlösbare diophantische Gleichungen*, J. Reine Angew. Math. **184** (1942), 12–18.

[Sch31] F. K. Schmidt, *Analytische Zahlentheorie in Körpern der Charakteristik p*, Math. Z. **33** (1931), 1–32.

[Sch07] A. Schmidt, *Einführung in die algebraische Zahlentheorie*, Springer, Berlin, 2007.

[SD04] P. Swinnerton-Dyer, *Diophantine equations: progress and problems*, Arithmetic of higher-dimensional algebraic varieties (Palo Alto, CA, 2002), Progr. Math., vol. 226, Birkhäuser Boston, Boston, MA, 2004, pp. 3–35.

[Ser73] J.-P. Serre, *A course in arithmetic*, Graduate Texts in Mathematics, vol. 7, Springer-Verlag, New York-Heidelberg, 1973.

[Sko42] T. Skolem, *Unlösbarkeit von Gleichungen, deren entsprechende Kongruenz für jeden Modul lösbar ist*, Avh. Norske Vid.-Akad. Oslo I (1942), no. 4, 28 pages.

[Wei48] A. Weil, *Sur les courbes algébriques et les variétés qui s'en déduisent*, Publications de l'Institut de Mathématiques de l'Université de Strasbourg, vol. 7 (1945), Hermann & Cie, Paris, 1948.