COUNTEREXAMPLES TO THE HASSE PRINCIPLE: AN ELEMENTARY INTRODUCTION

W. AITKEN, F. LEMMERMEYER

Abstract. We give a self-contained exposition concerning counterexamples to the Hasse principle. Our account, which uses only techniques from undergraduate number theory and algebra, focuses on counterexamples similar to the original ones discovered by Lind and Reichardt. As discussed in an appendix, this type of counterexample is important in the theory of elliptic curves: today they are interpreted as nontrivial elements in the Tate–Shafarevich group.

This is a version that has been adapted to Math 422 (CSUSM).

1. Introduction

The Diophantine equation

$$aX^2 + bY^2 + cZ^2 = 0 \tag{1}$$

has played a prominent role in the history of number theory.[1] We assume that a, b, and c are nonzero integers and, using a simple argument, we reduce to the case where the product abc is square-free. Lagrange (1768) solved the problem by giving a descent procedure which determines in a finite number of steps whether or not (1) has a nontrivial $\mathbb{Z}$-solution, but Legendre (1788) gave the definitive solution. Legendre proved that the following conditions, known by Euler to be necessary, are sufficient for the existence of a nontrivial $\mathbb{Z}$-solution: *(i) a, b, and c do not all have the same sign, and (ii) $-ab$ is a square modulo $|c|$, $-ca$ is a square modulo $|b|$, and $-bc$ is a square modulo $|a|$.* Legendre then made interesting use of this result in the first ever attempted proof of quadratic reciprocity.[2]

There was a large interest in generalizing Legendre's result to quadratic forms in arbitrary many variables. Hasse's solution (1923) was formulated in a very elegant way using the p-adic numbers developed earlier by his teacher Hensel.

---

[1] This equation is more general than it might at first appear. If $F \in \mathbb{Z}[X, Y, Z]$ is a homogeneous quadratic polynomial, then $F(X, Y, Z) = 0$ can be transformed to the form (1) (see [14, Thm. 1′, Ch. IV]). As a consequence, the problem of determining if a conic, defined over $\mathbb{Q}$, has a rational point reduces in a straightforward manner to the solvability of (1).

[2] The equation (1) figures prominently in the *Disquisitiones Arithmeticae* (1801) of Gauss [4, Articles 294–300]; Gauss proves Legendre's theorem using his theory of ternary quadratic forms and discusses the gaps in Legendre's proof of quadratic reciprocity.

For a proof of Legendre's theorem based on Lagrange's descent see [3, Chapter VII §3], [6, Chapter 17 §3], or [17, Chapter II §XIV, Chapter IV Appendix I] (which gives historical background including Lagrange's role in the solution to the problem). For more on Legendre's theorem see [9, Exercises 1.8, 2.36], and various books on Diophantine equations. Lagrange's descent gives an explicit method for finding a solution if it exists, see Cremona and Rusin [2] for practical improvements on the descent method.

To explain Hasse's result, we will need to fix some terminology. A *homogeneous polynomial* is a sum of monomials that are all of the same total degree; such polynomials are sometimes called *forms* of degree d. Consider the Diophantine equation

$$F(X_1, \dots, X_m) = 0 \tag{2}$$

where $F \in \mathbb{Z}[X_1, \dots, X_m]$ is a homogeneous polynomial of degree d. The m-tuple $(0, \dots, 0)$ is a solution, but not an interesting one. The m-tuple $(a_1, \dots, a_m)$ is called *nontrivial* if at least one a_i is nonzero. We are interested in finding necessary and sufficient conditions for the existence of nontrivial solutions to (2). A nontrivial m-tuple $(a_1, \dots, a_m) \in \mathbb{Z}^m$ is said to be *primitive* if the greatest common divisor of $a_1, \dots, a_m$ is 1. Observe that, by homogeneity and unique factorization, if (2) has any nontrivial solution (in $\mathbb{Z}^m$, or even $\mathbb{Q}^m$), it has a primitive solution. We extend this terminology in two ways: to systems of homogeneous polynomial equations, and to solutions modulo N. For example, a primitive solution modulo N is a primitive m-tuple that solves the congruence $F(X_1, \dots, X_m) \equiv 0$ modulo N.[3] (For systems, and systems modulo N, of homogeneous equations, we do not require that the equations have the same degree.)

An easy way to show that (2) has no nontrivial $\mathbb{Z}$-solution is to show that it has no nontrivial $\mathbb{R}$-solutions. This trick only eliminates the most blatant offenders: for any interesting Diophantine equation its nonsolvability will require some number-theoretic tools. The next easiest way to show that (2) has no nontrivial solution is to show that it fails to have a primitive solution modulo N for some N. What is surprising is that in degree 2 these two techniques are all that is needed.

Theorem (Hasse's Theorem: version 1)**.** *If $F \in \mathbb{Z}[X_1, \dots, X_m]$ is homogeneous of degree 2, then $F(X_1, \dots, X_m) = 0$ has a nontrivial $\mathbb{Z}$-solution if and only if*

(i) *it has a nontrivial $\mathbb{R}$-solution, and*
(ii) *it has a primitive solution modulo N for all positive integers N.*

The assertion that (i) and (ii) are necessary and sufficient for existence of nontrivial solutions is called the *Hasse principle* for polynomials of degree 2.

The Chinese remainder theorem allows us to restate this result as follows.

Theorem (Hasse's Theorem: version 2)**.** *If $F \in \mathbb{Z}[X_1, \dots, X_m]$ is homogeneous of degree 2, then $F(X_1, \dots, X_m) = 0$ has a nontrivial $\mathbb{Z}$-solution if and only if*

(i) *it has a nontrivial $\mathbb{R}$-solution, and*
(ii) *it has a primitive solution modulo p^k for all primes p and exponents $k \geq 1$.*

When a homogeneous Diophantine equation or system of such equations has primitive solutions modulo p^k for all powers p^k of a prime p we say that it is *p-locally solvable*. If it is p-locally solvable for every prime p and has nontrivial real solutions then we say that it is *locally solvable*, and if it has a nontrivial $\mathbb{Z}$-solution then we say that it is *globally solvable*. The above theorem states that, for a certain class of equations, global solvability is equivalent to local solvability.

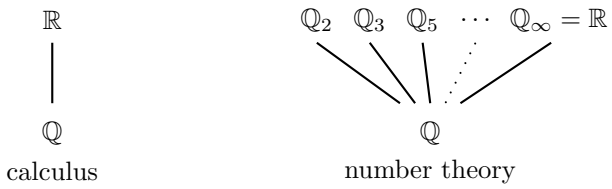
Example 1 ($m = 3$)**.** For Equation (1), Hasse's theorem is a consequence of Legendre's Theorem. See the exercises at the end of this section.

[3]Any m-tuple solving $F(X_1, \dots, X_m) \equiv 0 \bmod N$ that is nontrivial with GCD prime to N is congruent to a solution whose GCD is 1. Thus, if desired, one can relax the definition of *primitive m-tuple modulo N* to allow any nontrivial m-tuple whose GCD is prime to N.

Example 2 ($m = 2$)**.** For the equation $X^2 - aY^2 = 0$, Hasse's theorem is a consequence of quadratic reciprocity. (In fact, this equation has a nontrivial $\mathbb{Z}$-solution if and only if (i) $a \geq 0$, and (ii) it has a primitive solution modulo p for all primes p. This was stated in a slightly different form by Gauss in his *Disquisitiones* [4, Art. 125]. More generally for $a \geq 0$, it is true that $X^n - aY^n = 0$ has a nontrivial $\mathbb{Z}$-solution if and only if it has a nontrivial solution modulo p for all primes p for $n = 2, 3, \ldots, 7$. For $n = 8$, however, it is an easy exercise to check that $X^8 - 16Y^8 = 0$ does not have a nontrivial solution in $\mathbb{Z}$ although it has a primitive solution modulo p for all primes p. Hint: show that the congruence $X^8 - 16Y^8 \equiv 0$ does not have a primitive solution modulo 32. For a proof that the equation $X^8 - 16Y^8 = 0$ is in some sense the "most general" counterexample, see Kraft and Rosen [7].)

There are many situations where having a solution modulo p is enough to guarantee solutions modulo p^k for all exponents k. We will see examples of this phenomenon in this paper (and the above example shows a simple case where this does not occur). Although not needed for our main results, Hensel's lemma (see Appendix A) is the standard tool used to "lift" a solution modulo a prime p to a solution modulo p^k for arbitrary $k \geq 1$.

A natural setting for understanding solutions modulo p^k as k varies is through the *ring of p-adic integers* $\mathbb{Z}_p$ developed by Hensel. Using the ring $\mathbb{Z}_p$ allows one to organize a coherent sequence of solutions modulo p^k for infinitely many k into one p-adic solution. The field $\mathbb{Q}_p$ of p-adic numbers is the fraction field of $\mathbb{Z}_p$. The rings $\mathbb{Z}_p$ and fields $\mathbb{Q}_p$ play a crucial role in modern number theory, and are present in virtually every discussion of the Hasse principle. The current paper is somewhat exceptional: in order to make this paper more accessible, we do not use the p-adic numbers or Hensel's lemma. We direct the reader wishing to learn something about $\mathbb{Z}_p$ or Hensel's lemma to Appendix A. For now we mention that, like $\mathbb{R}$, the field $\mathbb{Q}_p$ is complete for a certain absolute value, and much of real or complex analysis generalizes to $\mathbb{Q}_p$. In fact, number theorists often formally introduce a "prime" ∞, and denote $\mathbb{R}$ by $\mathbb{Q}_\infty$; the fields $\mathbb{Q}_p$ for p a prime or ∞ give all the *completions* of $\mathbb{Q}$ and are called the *local fields* associated with $\mathbb{Q}$:



It is in this language that Hasse's theorem achieves its standard form.

Theorem (Hasse's Theorem: version 3)**.** *If $F \in \mathbb{Z}[X_1, \ldots, X_m]$ is homogeneous of degree 2, then $F(X_1, \ldots, X_m) = 0$ has a nontrivial $\mathbb{Q}$-solution if and only if it has a nontrivial $\mathbb{Q}_p$-solution for all p (including $p = \infty$).*

We say that a class of homogeneous equations satisfies the *Hasse principle* if each equation in the class has a nontrivial $\mathbb{Z}$-solution if and only if (*i*) it has a $\mathbb{R}$-solution, and (*ii*) it has a primitive solution modulo N for each N. As mentioned above, the Chinese remainder theorem allows us to replace (*ii*) by the following: (*ii'*) it has a

primitive solution modulo p^k for each prime p and exponent $k \geq 1$. We formulate the Hasse principle for systems of homogeneous polynomials in a similar manner.[4]

However, *the Hasse principle fails in general.* In fact, it fails for the next obvious class of equations: cubic equations. The most famous example is due to Selmer [13]:

$$3X^3 + 4Y^3 + 5Z^3 = 0. \tag{3}$$

This cubic obviously has nontrivial $\mathbb{R}$-solutions, and it can be shown to have solutions modulo each prime power but *it has no nontrivial $\mathbb{Z}$-solutions.*[5]

What if one sticks to quadratic equations, but allow *systems* of equations? In this paper we will show that the Hasse principle also fails for this class. In particular we study systems of the form

$$aU^2 + bV^2 + cW^2 = dZ^2, \qquad UW = V^2. \tag{4}$$

and use completely elementary methods to produce counterexamples to the Hasse principle.[6] The case where $a = 1, b = 0, c = -17, d = 2$ is important in the history of the Hasse Principle since it was the first known counterexample to the Hasse principle for diophantine equations[7] It was produced by Lind [10] and Reichardt [12] several years before Selmer's. As we will discuss in Section 6, the system (4) can be transformed into the single (nonhomogeneous) equation

$$X^4 - 17Y^4 = 2Z^2 \tag{5}$$

which was the form considered by Lind and Reichardt. In contrast to Selmer's example, there are proofs, like the one given in the current paper, that (5) has no nontrivial $\mathbb{Z}$-solutions involving only quadratic reciprocity — and there are proofs (see [8]) that require even less. The harder part is to give a completely elementary proof that (5) has solutions modulo all primes.[8]

The purpose of this article is to give a self-contained, accessible proof of the existence of counterexamples to the Hasse principle of the form (4), counterexamples

[4]Obviously this is equivalent to the usual formulation of the Hasse principle in terms of nontrivial $\mathbb{Q}_p$-solutions (including $p = \infty$). The Hasse principle is also known as the *local-global principle*: a $\mathbb{Q}_p$-solution is considered a *local solution*, and a $\mathbb{Q}$-solution is called a *global solution.*

We formulate the Hasse principle for homogeneous equations in order to restrict our attention to integer solutions. In the language of algebraic geometry, this formulation asserts the existence of $\mathbb{Q}$-points on the associated projective variety given the existence of $\mathbb{Q}_p$-points for all p.

[5]Showing the absence of integral solutions is not elementary. Known proofs of this fact use the arithmetic of cubic number fields; one possible approach is to multiply (3) through by 2 and factor the left-hand side of the transformed equation $6X^3 + Y^3 = 10Z^3$ over $\mathbb{Q}(\sqrt[3]{6})$.

This work of Selmer led Cassels to introduce the notion of Selmer groups and to his groundbreaking work on Tate–Shafarevich groups in the theory of elliptic curves; nowadays, Selmer's example can be interpreted as representing an element of order 3 in the Tate–Shafarevich group Ш_E of the elliptic curve $E : X^3 + Y^3 + 60Z^3 = 0$. See [1], [11], and our Appendix B for more on the relationship between counterexamples and the Tate–Shafarevich group.

[6]In the main body of the paper we consider only the case where $b = 0$, but as discussed in Appendix B, the general case is important in the study of eliptic curves.

[7]Counterexamples to the Hasse principle for norms, according to which an element of a number field is a norm if and only if it is a norm in every localization, were known for noncyclic extensions already around 1934.

[8]Aside from the current paper, the most elementary approach uses quartic Gauss and Jacobi sums. Applied to quartics like $aX^4 + bY^4 = Z^2$ this method only shows the solvability for sufficiently large values of p, and making the bounds explicit is quite technical.

Short, if less elementary, arguments can be given if one uses the Hasse-Weil bounds for curves of genus 1 defined over finite fields, or F. K. Schmidt's result on the existence of points on genus 1 curves over finite fields.

similar to those of Lind and Reichardt's, using the easy and well-known technique of parametrizing conics. In fact, the only required background is a standard undergraduate course in number theory up to quadratic reciprocity, and a standard undergraduate course in modern algebra up to basic facts about polynomials over rings and fields.[9] As far as we know, this paper is unique in developing interesting counterexamples to the Hasse principle in such an elementary manner.[10] We hope that this paper will give a general mathematical audience a taste of this interesting subject.

Variants of the Hasse principle, and the study of the manner in which these principles fail is a very important and active area of current research.[11] As discussed in Appendix B, these counterexamples are of interest from the point of view of elliptic curves.

We conclude this introduction by offering exercises showing the relationship between Legendre's theorem, discussed at the start of this introduction, and the Hasse principle. As above, assume that $a, b, c \in \mathbb{Z}$ are such that abc is a nonzero and square-free.

Exercise 1. Let p be a prime. Call (x_0, y_0, z_0) a *p-strong* triple if at most one of x_0, y_0, z_0 is divisible by p. Show that any primitive solution to the congruence

$$aX^2 + bY^2 + cZ^2 \equiv 0 \bmod p^2$$

is p-strong.

Exercise 2. Suppose that $p \mid a$ and that the congruence $aX^2+bY^2+cZ^2 \equiv 0 \bmod p$ has a p-strong solution. Show that $-bc$ is a square modulo p.

Conclude that if $aX^2 + bY^2 + cZ^2 \equiv 0 \bmod p$ has a p-strong solution for all odd $p \mid a$, then $-bc$ is a square modulo $|a|$.

Exercise 3. Take Legendre's theorem as given and use the preceding exercise to show that if the congruence $aX^2 + bY^2 + cZ^2 \equiv 0 \bmod p$ has a p-strong solution for all odd primes $p \mid abc$, and if the equation $aX^2 + bY^2 + cZ^2 = 0$ has a nontrivial $\mathbb{R}$-solution, then $aX^2 + bY^2 + cZ^2 = 0$ has a nontrivial $\mathbb{Z}$-solution.

Exercise 4. Use the above exercises to show that the Hasse principle for the equation $aX^2 + bY^2 + cZ^2 = 0$ is a consequence of Legendre's theorem.

2. Parametrizing Conics

A standard method for finding Pythagorean triples is through the rational parametrization of the unit circle $\{(x, y) \in \mathbb{R}^2 \mid x^2 + y^2 = 1\}$. The parametrization is found by intersecting the circle with the line of slope t going through the point $P = (-1, 0)$ of the circle. The line defined by $y = t(x + 1)$ intersects the circle defined by $x^2 + y^2 - 1 = 0$ at points whose first coordinates satisfy the equation

[9] Comments directed to a more advanced audience will be confined to the footnotes and the appendices.

[10] A less interesting, but simpler counterexample is $(X^2 - 2Y^2)(X^2 - 17Y^2)(X^2 - 34Y^2) = 0$. To find solutions modulo p^k, use properties of the Legendre symbol, and Propositions 1 and 2.

[11] See Mazur [11] or the summary of mini-courses by Colliot-Thélène and others at

`http://swc.math.arizona.edu/oldaws/99GenlInfo.html`

for some recent examples.

$0 = x^2 + t^2(x+1)^2 - 1 = (x+1)(x-1+t^2x+t^2)$. The points of intersection are the point $P = (-1, 0)$ we started with, as well as $P_t = \left(\frac{1-t^2}{1+t^2}, \frac{2t}{1+t^2}\right)$.

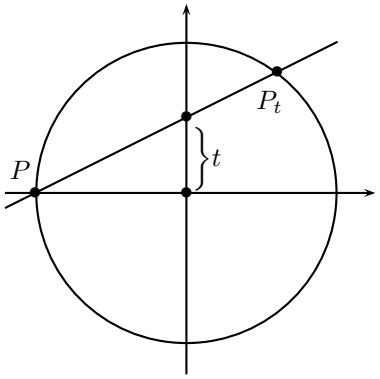


FIGURE 1. Parametrizing the Unit Circle

This parametrization leads us to the following identity in $\mathbb{R}[T]$:

$$(1-T^2)^2 + (2T)^2 = (1+T^2)^2. \tag{6}$$

Specializing T to n/m with $n, m \in \mathbb{Z}$ gives Pythagorean triples:

$$(m^2-n^2)^2 + (2mn)^2 = (m^2+n^2)^2.$$

The above procedure is purely algebraic, and there is no problem modifying it to the equation $ax^2 + by^2 = 1$ over a general field F where $a, b \in F$ are nonzero. Of course, we need a starting point: we need $x_0, y_0 \in F$ such that $ax_0^2 + by_0^2 = 1$. The analogue to (6) is displayed in the following lemma as (7).[12]

Lemma 1. *Let F be a field, and let $a, b \in F$ be nonzero. Let $x_0, y_0 \in F$ be such that $ax_0^2 + by_0^2 = 1$. Then in $F[T]$*

$$aq_1^2 + bq_2^2 = q_3^2 \tag{7}$$

where

$$q_1 = bx_0T^2 - 2by_0T - ax_0, \quad q_2 = -by_0T^2 - 2ax_0T + ay_0, \quad q_3 = bT^2 + a.$$

Furthermore, at least two of q_1, q_2, q_3 have degree exactly 2. Finally, if $\operatorname{char} F \neq 2$*, each of q_1, q_2, q_3 is nonzero, and no two are associates.*[13]

Proof. The polynomials q_1, q_2, q_3 are found using the parametrization method, but how they are discovered is not crucial to the proof. What is important is that $aq_1^2 + bq_2^2 = q_3^2$, which is verified with a straightforward calculation. Observe that $\deg q_3 = 2$ since $b \neq 0$. Since $q_3^2 = aq_1^2 + bq_2^2$, we also have $\deg q_1 = 2$ or $\deg q_2 = 2$.

Assume $\operatorname{char} F \neq 2$. Since a and b are nonzero, and x_0 and y_0 are not both 0, each of q_1, q_2, q_3 is nonzero. Suppose two of q_1, q_2, q_3 are associates. Then these two must have degree 2. The equation $aq_1^2 + bq_2^2 = q_3^2$ then implies q_1, q_2, q_3 are

[12]In the language of algebraic geometry, a nonsingular plane conic possessing at least one F-rational point is isomorphic to $\mathbb{P}^1$ via such a parametrization. The restriction to conics of the form $ax^2 + by^2 = 1$ is not a true restriction: if $\operatorname{char} F \neq 2$ then every nondegenerate conic can be brought into the form $ax^2 + by^2 = 1$ with a projective transformation.

[13]Recall that two nonzero polynomials of $F[T]$ are associates if one is a constant multiple of the other. More generally, in any unique factorization domain, two non-zero elements are called *associates* if the second is the product of a unit with the first.

all associates. By Lemma 2 below, q_1, q_2 are constant multiplies of q_3. But this contradicts the fact that at least one of q_1 or q_2 has a nonzero linear term. □

The above makes use of the following general fact:

Lemma 2. *Let a and b be nonzero elements of a unique factorization domain R. If a^n and b^n are associates for some positive n, then a and b are associates.*

Proof. Factor a and b into irreducible elements. Up to multiplication by units, a^n and b^n have the same factorization. This means that a and b must also have the same factorization up to multiplication by units. □

The existence of q_1, q_2, q_3 in the above lemma depends on the existence of at least one solution $ax_0^2 + by_0^2 = 1$. For $F = \mathbb{F}_p$ the existence of such a solution follows from Euler's criterion.[14]

Lemma 3. *Let a and b be nonzero elements of the field $\mathbb{F}_p$ where p is a prime. Then there exist $x_0, y_0 \in \mathbb{F}_p$ such that $ax_0^2 + by_0^2 = 1$.*

Proof. If $p = 2$, take $x_0 = 1$ and $y_0 = 0$. If $p > 2$, we wish to solve $y^2 = f(x)$ where $f(x) = b^{-1}(1 - ax^2)$. If there are no solutions, then $f(t)$ is a nonsquare for each $t \in \mathbb{F}_p$. By Euler's criterion, $f(t)^{(p-1)/2} = -1$ for all $t \in \mathbb{F}_p$. However, this contradicts the fact that the degree $p - 1$ polynomial $f(x)^{(p-1)/2} + 1$ has at most $p - 1$ roots. □

Remark. This result is due to Euler and arose from his attempt to prove Fermat's claim that every integer is the sum of four squares, a theorem finally proved by Lagrange (see [17, Chapter III §XI]). For that theorem, one uses the solvability of $-x^2 - y^2 = 1$ in $\mathbb{F}_p$.

Remark. As we have seen, methods for parametrizing the unit circle turn out to apply to conics defined over general fields. This is an example of a major theme of arithmetic geometry, that many ideas of geometry carry over to other fields of interest to number theorists. The reader might be amused to see a further example. Figure 2 displays the plane over $\mathbb{F}_7$ which has 7^2 points, denoted by $+$ or $\bullet$, and the unit circle $x^2 + y^2 = 1$ consisting of 8 points, denoted by $\bullet$. In the graph on the right, the line $L : y = x + 3$ is displayed. Note that every line in the affine plane over $\mathbb{F}_7$ contains 7 points – the dots between, say, $(0, 3)$ and $(1, 4)$ are not part of the line, and are only drawn to help you visualize the line. We also remark that L can also be written as $y = -6x + 3$; this changes the appearance of the dots between the points, but, of course, not the points on L. The line L intersects the unit circle in exactly one point, namely $(2, 5)$, hence is the tangent to the unit circle at this point. Similarly, $x = 1$ is the tangent to the unit circle at $(1, 0)$. The line $y = 2x - 1$ intersects the unit circle in exactly two points: can you see which?

[14]Suppose p is an odd prime and $a \in \mathbb{F}_p$ is non-zero. Euler's criterion states that a is a square in the field $\mathbb{F}_p$ if and only if $a^{(p-1)/2} = 1$, and that a is not a square in $\mathbb{F}_p$ if and only if $a^{(p-1)/2} = -1$. Euler's criterion is a consequence of the well-known result that the multiplicative group of non-zero elements of $\mathbb{F}_p$ is cyclic of order $p - 1$.

In fact, the multiplicative group $F^\times$ of any finite field F is cyclic. Thus Euler's criterion generalizes to any finite field F of odd order. One can also use the cyclic nature of $F^\times$ to show that every element of a finite field of even order is a square. As a consequence, Lemma 3 generalize to arbitrary finite fields.

We leave it as an exercise to the reader to determine the interior of the unit circle: these are defined to be the points that do not lie on any tangent to the circle. For example, the points $(1, x)$ with $1 \le x \le 6$ are exterior points since they lie on the tangent at $(1, 0)$.

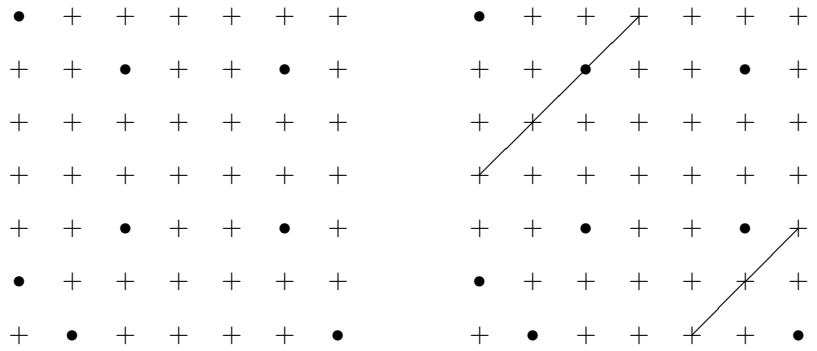


FIGURE 2. The unit circle over $\mathbb{F}_7$, and its tangent at $(2, 5)$

3. Solutions modulo odd primes

Let p be an odd prime. We now turn our attention to finding nontrivial solutions of the system

$$aU^2 + cW^2 = dZ^2, \qquad UW = V^2$$

with values in $F = \mathbb{F}_p$. Here $a, c, d \in \mathbb{F}_p$ are assumed nonzero.

Replacing a and c with ad^{-1} and cd^{-1} we can assume $d = 1$. The first equation $aU^2 + cW^2 = Z^2$ can be parametrized as in Section 2. This gives a whole family of solutions to the first equation, and we need to determine that at least one of these solutions also satisfies $UW = V^2$. The following is a key ingredient to doing so.[15]

Lemma 4. *Let $f, g \in \mathbb{F}_p[X]$ be nonzero polynomials of degree at most two. If $\left(\frac{f(t)}{p}\right) = \left(\frac{g(t)}{p}\right)$ for all $t \in \mathbb{F}_p$, or if $\left(\frac{f(t)}{p}\right) = -\left(\frac{g(t)}{p}\right)$ for all $t \in \mathbb{F}_p$, then f and g are associates.*

Remark. The statement of this result uses the *Legendre symbol* $\left(\frac{a}{p}\right)$. If $a \in \mathbb{F}_p$ then the Legendre symbol can be defined as follows:

$$\left(\frac{a}{p}\right) = \begin{cases} 1 & \text{if } a \text{ is a nonzero square in } \mathbb{F}_p \\ -1 & \text{if } a \text{ is not a square in } \mathbb{F}_p \\ 0 & \text{if } a = 0 \text{ in } \mathbb{F}_p \end{cases}$$

The Legendre symbol provides a convenient notation for the expression of theorems such as quadratic reciprocity or the simpler theorem that $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$. This last equation is a consequence of Euler's criterion:

$$a^{(p-1)/2} = \left(\frac{a}{p}\right)$$

(where we view the values $0, 1, -1$ of the Legendre symbol as elements of $\mathbb{F}_p$. Recall p is an odd prime, so $0, 1, -1$ are distinct.)

[15]Everything in this section extends easily to finite fields of odd order, not just prime fields.

Proof. By Euler's criterion, $\left(\frac{f(t)}{p}\right) = f(t)^{(p-1)/2}$ and $\left(\frac{g(t)}{p}\right) = g(t)^{(p-1)/2}$. So, if $\left(\frac{f(t)}{p}\right) = \left(\frac{g(t)}{p}\right)$ for all $t \in \mathbb{F}_p$, then every $t \in \mathbb{F}_p$ is a root of $f^{(p-1)/2} - g^{(p-1)/2}$. Recall that a nonzero polynomial in $\mathbb{F}_p[T]$ of degree d has at most d roots. This follows from the fact that $\mathbb{F}_p$ is a field. The polynomial $f^{(p-1)/2} - g^{(p-1)/2}$ has degree at most $p-1$, but has p roots. We conclude that $f^{(p-1)/2} - g^{(p-1)/2}$ is the zero polynomial.

Since $\mathbb{F}_p[X]$ is a unique factorization domain, and since $f^{(p-1)/2} = g^{(p-1)/2}$, the polynomials f and g are associates by Lemma 2.

If $\left(\frac{f(t)}{p}\right) = -\left(\frac{g(t)}{p}\right)$ for all $t \in \mathbb{F}_p$, pick a nonsquare r in $\mathbb{F}_p$. Observe that $\left(\frac{f(t)}{p}\right) = \left(\frac{rg(t)}{p}\right)$ for all $t \in \mathbb{F}_p$, so f and rg are associates by the conclusion of the previous case. In particular, f and g are associates. □

Theorem 1. *Let p be an odd prime, and let $a, c, d \in \mathbb{F}_p$ be nonzero. Then the system*

$$aU^2 + cW^2 = dZ^2, \qquad UW = V^2$$

has a nontrivial $\mathbb{F}_p$-solution.

Proof. As mentioned above, we reduce to the case $d = 1$. Parametrizing the conic $aU^2 + cW^2 = Z^2$ as in Lemma 1 (and Lemma 3) yields nonzero polynomials $q_1, q_2, q_3 \in \mathbb{F}_p[T]$ where $aq_1^2 + cq_2^2 = q_3^2$ and where q_1 and q_3 are not associates.

By Lemma 4 and the fact that q_1 and q_2 are not associates, there is a $t \in \mathbb{F}_p$ such that $\left(\frac{q_1(t)}{p}\right) \neq -\left(\frac{q_2(t)}{p}\right)$. So $q_1(t)$ and $q_2(t)$ are not both zero and $\left(\frac{q_1(t)q_2(t)}{p}\right) \neq -1$. Thus $q_1(t)q_2(t) = v^2$ for some $v \in \mathbb{F}_p$. Hence $U = q_1(t), W = q_2(t), Z = q_3(t)$, $V = v$ is a nontrivial solution. □

4. Solutions modulo prime powers

Now we focus on the solvability of the system

$$aU^2 + cW^2 = dZ^2, \qquad UW = V^2 \tag{8}$$

where a, c, d are nonzero integers. A consequence of Theorem 1 is that if p is an odd prime and if $p \nmid acd$ then this system has a primitive solution modulo p. In this section we extend this result to powers of p. We also discuss the case of $p = 2$.

For the convenience of the reader, we state and prove the following well-known result from elementary number theory.

Proposition 1. *Let p be a prime and let N and $r > 0$ be integers such that $p \nmid rN$. If N is an rth power modulo p, then N is an rth power modulo p^k for all $k \geq 1$.*

Proof. (Induction on k). Suppose that $N \equiv a^r \bmod p^k$. Write $N = a^r + cp^k$, and let x be a solution to $ra^{r-1}x \equiv c \bmod p$. Using the binomial expansion,

$$(a + xp^k)^r \equiv a^r + ra^{r-1}xp^k \equiv a^r + cp^k \mod p^{k+1}.$$

□

We now consider the main result of this section. A *strong solution*[16] modulo p^k to the system (8) is a primitive solution (u, v, w, z) to the associated congruences modulo p^k such that at least one of au, cw, dz is nonzero modulo the prime p.

[16]This notion of strong is not that of the exercises of Section 1.

Theorem 2. *Let p be an odd prime, and let a, c, d be nonzero integers. If*

$$aU^2 + cW^2 = dZ^2, \qquad UW = V^2$$

has a strong solution modulo p, then it has a strong solution modulo p^k for all k. In particular, it is p-locally solvable.

Proof. Let (u_0, v_0, w_0, z_0) be a strong solution modulo p. Since $au_0^2 + cw_0^2 = dz_0^2$, at least two of au_0, cw_0, dz_0 must be nonzero modulo p. By symmetry we can assume that au_0 is nonzero modulo p. Fix a power p^k of p. Since $p \nmid a$ and $p \nmid u_0$, we can choose $a^{-1}, u_0^{-1} \in \mathbb{Z}$ which are inverses to a and u_0 modulo p^k.

Let $v = v_0\, u_0^{-1}$, $w = w_0\, u_0^{-1}$, and $z = z_0\, u_0^{-1}$. Then $(1, v, w, z)$ also solves the system modulo p. So $w \equiv v^2 \bmod p$, and hence $a + cv^4 \equiv dz^2 \bmod p$. Since $a^{-1}\left(dz^2 - cv^4\right) \equiv 1 \bmod p$, and since 1 is a fourth power, Proposition 1 guarantees the existence of an $m \in \mathbb{Z}$, such that $a^{-1}\left(dz^2 - cv^4\right) \equiv m^4 \bmod p^k$. In other words, $am^4 + cv^4 \equiv dz^2 \bmod p^k$, so (m^2, mv, v^2, z) is a solution modulo p^k. It is a strong solution since m is nonzero modulo p. □

Theorem 2 together with Theorem 1 yield the following:

Corollary 1. *If p be an odd prime such that $p \nmid acd$ then*

$$aU^2 + cW^2 = dZ^2, \qquad UW = V^2$$

is p-locally solvable: it has primitive solutions modulo p^k for all k.

For $p = 2$ the situation is more subtle. For example, the system

$$U^2 + 3W^2 = 7Z^2, \qquad UW = V^2$$

has solution $(1, 1, 1, 2)$ modulo 2. In fact, $(1, 1, 1, 2)$ is a solution modulo 2^3. However, the system has no primitive solution modulo 2^4. The following exercise provides a shortcut for verifying this claim.

Exercise 5. Consider the system $aU^2 + cW^2 = dZ^2$, $UW = V^2$ where $a, c, d \in \mathbb{Z}$ are odd. Show that if there is a primitive solution modulo 16, then there is a solution (u, v, w, z) with $u, v, w \in \{0, 1\}$ and $z \in \{0, 1, 2, 3\}$.

A difficulty with extending Theorem 2 to $p = 2$ is the limitations of Proposition 1: the integer 3 is a fourth power modulo $p = 2$ but not modulo 2^k if $k > 1$. The following provides the needed variant to Proposition 1.

Proposition 2. *If $N \equiv 1 \bmod 2^4$, then N is a fourth power modulo 2^k for all $k \geq 1$.*

Proof. (Induction on k). Suppose $N \equiv a^4 \bmod 2^k$ where $k \geq 4$. Write $N = a^4 + c2^k$. Using the binomial expansion and the fact that $a^3 \equiv 1 \bmod 2$,

$$(a + c2^{k-2})^4 \equiv a^4 + 4a^3 c2^{k-2} \equiv a^4 + c2^k \mod 2^{k+1}.$$

□

Using this we can prove the following. Its proof is similar to that of Theorem 2.

Theorem 3. *Let a, c, d be nonzero integers. If the system*

$$aU^2 + cW^2 = dZ^2, \qquad UW = V^2$$

has a strong solution modulo 2^4, then it has a strong solution modulo 2^k for all k.

In some cases there is no distinction between primitive solutions and strong solutions:

Lemma 5. *Suppose p is a prime, $k \geq 2$, and $a, c, d \in \mathbb{Z}$ are such that $p^2 \nmid acd$. Then every primitive solution to (8) modulo p^k is a strong solution.*

Proof. Let (u, v, w, z) be a primitive solution modulo p^k that is not a strong solution. We derive a contradiction in the case where $p \nmid u$; the other cases are similar. Since (u, v, w, z) is not a strong solution, $p \mid a$. Thus $p \nmid cd$. So p divides both w and z since (u, v, w, z) is not a strong solution. Looking at $au^2 + cw^2 \equiv dz^2$ modulo p^2 gives us that $au^2 \equiv 0 \bmod p^2$. Thus $p^2 \mid a$, a contradiction. □

Corollary 2. *Let p be a prime, and let a, c, d be integers such that $p^2 \nmid acd$. If p is odd then the system (8) is p-locally solvable if and only if it possesses a strong solution modulo p. If $p = 2$, the system is p-locally solvable if and only if it possesses a strong solution modulo 2^4.*

Proof. One direction follows from Theorems 2 and 3. For the other direction, suppose (8) is p-locally solvable. So there is a primitive solution modulo p^4. By Lemma 5, there is a strong solution modulo p^4. For the case where p is odd, observe that such a solution is also a strong solution modulo p. □

The general case where p^2 is allowed to divide acd will be taken up in Section 6.

5. Counterexamples to the Hasse principle

The goal of this section is to identify counterexamples to the Hasse principle. These are systems that are locally solvable, but not globally solvable: they lack nontrivial $\mathbb{Z}$-solutions.

We start with the question of local solvability.

Proposition 3. *Suppose*

1. *q and d are relatively prime nonzero integers and q is positive,*
2. *$q \equiv 1 \bmod 16$,*
3. *d is a square modulo p for all odd $p \mid q$, and*
4. *q is a fourth power modulo p for all odd $p \mid d$.*

Then the following system is locally solvable:

$$U^2 - qW^2 = dZ^2, \qquad UW = V^2$$

Proof. Observe that $(u, v, w, z) = \left(q^{1/2}, q^{1/4}, 1, 0\right)$ is a real solution. For all $p \nmid 2qd$, the system is p-locally solvable by Corollary 1. Observe that $(u, v, w, z) = (1, 1, 1, 0)$ is a strong solution modulo 16. By Theorem 3, the system is 2-locally solvable.

Suppose $p \mid q$ is odd. Let m be such that $m^2 \equiv d \bmod p$. Then $(u, v, w, z) = (m, 0, 0, 1)$ is a solution modulo p. Since d and q are relatively prime, $p \nmid d$. Thus the solution is strong. By Theorem 2, the system is p-locally solvable.

Suppose $p \mid d$ is odd. Let m be such that $m^4 \equiv q \bmod p$. Then $(u, v, w, z) = (m^2, m, 1, 0)$ is a modulo p solution. The solution is strong since $p \nmid q$. By Theorem 2, the system is p-locally solvable. □

Now we will find systems that have no nontrival $\mathbb{Z}$-solutions. Our examples will rely on the following key lemma:

Lemma 6. *Let d be a nonzero square-free integer, and let $q \equiv 1 \bmod 8$ be a prime not dividing d. If the system $U^2 - qW^2 = dZ^2$, $UW = V^2$ has a nontrivial $\mathbb{Z}$-solution, then d is a fourth power modulo q.*

Proof. Since the system is homogeneous, it has a primitive solution (u, v, w, z). Observe that u and w must be relatively prime since d is square-free: if $p \mid u$ and $p \mid w$ then $p \mid v$ and $p^2 \mid dz^2$, so $p^2 \mid d$ a contradiction. A similar argument shows that u and z are relatively prime, and w and z are relatively prime. Also, since $u^2w^2 = v^4$ and u, w are relatively prime, u^2 and w^2 must be fourth powers.

Let p be an odd prime dividing z. Modulo p we have $u^2 \equiv qw^2$. Let w^{-1} be an inverse to w modulo p. So $q \equiv \left(uw^{-1}\right)^2 \bmod p$. In terms of the Legendre symbol: $(\frac{q}{p}) = 1$. Since $q \equiv 1 \bmod 4$, quadratic reciprocity tells us that $(\frac{p}{q}) = 1$.

Thus $(\frac{p}{q}) = 1$ for all odd $p \mid z$. Since $q \equiv 1 \bmod 8$ we also have $(\frac{2}{q}) = 1$ and $(\frac{-1}{q}) = 1$. By the multiplicativity of the Legendre symbol it follows that $(\frac{z}{q}) = 1$. Thus z^2 is a nonzero fourth power modulo q.

We have that $u^2 \equiv dz^2 \bmod q$. We know that u^2 and z^2 are fourth powers modulo q. It follows that d is a fourth power modulo q. □

Now consider the system of homogeneous Diophantine equations

$$U^2 - qW^2 = dZ^2, \qquad UW = V^2 \tag{9}$$

where

(1) q is a prime such that $q \equiv 1 \bmod 16$,
(2) d is nonzero, square-free, and not divisible by q,
(3) d is a square, but not a fourth power, modulo q, and
(4) q is a fourth power modulo p for every odd p dividing d.

Proposition 3 and Lemma 6 together gives us our main result.

Theorem 4. *The system* (9) *is locally solvable but not globally solvable: it has no nontrivial $\mathbb{Z}$-solutions.*

We end with a few specific examples of (9).

Example 3. Lind and Reichardt's example, the first known counterexample to the Hasse principle, is the following special case of Theorem 4:

$$U^2 - 17W^2 = 2Z^2, \qquad UW = V^2.$$

This is a counterexample since 2 is a square, but not a fourth power, modulo 17. This example is often stated in terms of the equation $X^4 - 17Y^4 = 2Z^2$ (see Section 6).

Example 4. More generally, let q be a prime such that $q \equiv 1 \bmod 16$ and such that 2 is not a fourth power modulo q. In this case $(\frac{2}{q}) = 1$, so

$$U^2 - qW^2 = 2Z^2, \qquad UW = V^2$$

gives a counterexample to the Hasse principle.[17]

Example 5. For an example where $d \neq 2$, consider

$$U^2 - 17W^2 = 19Z^2, \qquad UW = V^2.$$

[17]Actually, we need only assume $q \equiv 1 \bmod 8$ since $(1, 1, 1, 2)$ is a strong solution modulo 16 if $q \equiv 9 \bmod 16$. Also we note that this family of examples is infinite. In fact, the density of primes q with $q \equiv 1 \bmod 8$ such that 2 is not a fourth power modulo q is $1/8$. This can be seen by applying the Chebotarev density theorem to the extension $\mathbb{Q}(\sqrt[4]{2}, i)/\mathbb{Q}$, whose Galois group is the dihedral group of order 8.

6. Further Issues

We conclude by addressing two issues raised earlier. The first concerns the extension of Corollary 2 to the case where $p^2 \mid abc$. The second concerns the relationship between the systems studied in this paper and the Diophantine equation $aX^4 + bX^2Y^2 + cY^4 = dZ^2$ studied by others.

Local Solvability. Corollary 2 gives necessary and sufficient conditions for the p-local solvability of the system $aU^2 + cW^2 = dZ^2,\ \ UW = V^2$ when $p^2 \nmid abc$. These conditions give a computationally effective procedure for deciding p-local solvability. In fact, Corollary 2 and Corollary 1 together yield a computationally effective procedure for deciding local solvability as a whole, at least if $p^2 \nmid abc$. We will now discuss an effective procedure for deciding p-local solvability even when $p^2 \mid abc$. By Corollary 1 this implies that local solvability is effectively decidable (deciding $\mathbb{R}$-solvability is easy).

We begin with some terminology. Given nonzero integers a, c, d we refer to the system $aU^2 + cW^2 = dZ^2,\ \ UW = V^2$ as the *system with coefficients* (a, c, d). We write $(a, c, d) \sim (a', c', d')$ is the two systems are both are p-locally solvable or neither is.

Lemma 7. *Let $a, c, d \in \mathbb{Z}$ be nonzero integers and let p be a prime. Then*

$$(a, c, d) \sim (c, a, d) \sim (pa, pc, pd) \sim \left(ap^2, cp^2, d\right)$$
$$\sim \left(a, c, dp^2\right) \sim \left(ap^4, c, d\right) \sim \left(a, cp^4, d\right).$$

Proof. We show that the p-local sovability of (a, c, d) implies that of $\left(ap^4, c, d\right)$. The proofs of the other implications are similar.

Suppose (u, v, w, z) is a primitive solution modulo p^k to system with coefficients (a, c, d). Then (u, pv, p^2w, p^2z) is a solution modulo p^{k+2} to the system with coefficients $\left(ap^4, c, d\right)$. If this solution is not primitive, divide each coordinate by the largest common power of p (either p or p^2) to obtain a primitive solution modulo p^{k-2} to the system with coefficients $\left(ap^4, c, d\right)$. □

We now apply Lemma 7 for showing that $(a, c, d) \sim (a', c', d')$ with $p \nmid a'$. To this end, we apply $(pa, pc, pd) \sim (a, c, d)$ until one of the coefficients is coprime to p. We can make sure that $p \nmid a$ by observing that $(a, c, d) \sim (c, a, d)$ and $(pa, pc, d) \sim (pa, pc, p^2d) \sim (a, c, pd)$. Applying $(a, p^4c, d) \sim (a, c, d)$ and $(a, c, p^2d) \sim (a, c, d)$ we end up with a system (a, c, d) satisfying $p \nmid a$, $p^4 \nmid c$ and $p^2 \nmid d$.

We can go further.

Lemma 8. *Let (a, c, d) be a system with $p \nmid a$, $p^4 \nmid c$ and $p^2 \nmid d$. If $c = c_0p^2$ and $d = d_0p$, where $p \nmid c_0d_0$, then the system is not p-solvable. In all other cases, (a, b, c) is equivalent to a system in which at most one coefficient is divisible by p.*

Proof. Suppose a system (a, p^2c_0, pd_0) with $p \nmid ac_0d_0$ has a primitive solution (u, v, w, z) modulo p^4. From $au^2 + p^2c_0w^2 \equiv pd_0z^2$ modulo p^4, it follows that $p \mid u$, which in turn implies $p \mid z$. Also $p \mid v$ so $p \nmid w$ (the solution is primitive). From $p^2 \mid u$, it follows that $p^3 \mid p^2c_0w^2$, a contradiction.

Finally, $(a, p^3c, pd) \sim (p^4a, p^3c, pd) \sim (p^3a, p^2c, d) \sim (p^3a, p^2c, p^2d) \sim (pa, c, d) \sim (c, pa, d)$, and similarly we find $(a, pc, pd) \sim (c, p^3a, d)$. □

The following lemmas give computationally effective tests to determine p-local solvability for the remaining systems.

Lemma 9. *The systems (a,c,d), (a,cp,d), (a,c,dp), and (a,cp^3,d) with $p\nmid acd$ are p-locally solvable if and only if they have strong solutions modulo p if p is odd, or modulo 16 if $p=2$.*

Proof. This follows from Corollary 2 if the system is one of the first three. So we assume that the coefficients are (a,cp^3,d) where a,c,d are prime to p.

First suppose the system is p-locally solvable, and let (u,v,w,z) be a primitive solution modulo p^4. If (u,v,w,z) is not strong, then $p\mid u$ and $p\mid z$. This forces $p\nmid w$ since (u,v,w,z) is primitive. Since $p\mid v$, we have $p^2\mid u$. So, $dz^2\equiv 0$ modulo p^3. Thus $p^2\mid z$. Modulo p^4 we now have $cp^3w^2\equiv 0$, contradicting the fact that c and w are prime to p. Thus (u,v,w,z) must be a strong solution modulo p^4.

So if the system is p-locally solvable it possesses a strong solution modulo p^4, and hence modulo p. The converse follows from Theorems 2 and 3. □

Lemma 10. *The system (a,cp^2,d) with $p\nmid acd$ is p-locally solvable if and only if*

(i) *it has a strong solution modulo m, or*
(ii) *the system with coefficients (ap^2,c,d) has a strong solution modulo m.*

Here $m=p$ if p is odd, but $m=16$ if $p=2$.

Proof. Suppose p-local solvability holds, and let (u,v,w,z) be a primitive solution modulo p^6. If $p\nmid u$, the solution is strong. Suppose $p\mid u$. This implies that $v^2\equiv 0$ and $d_0z^2\equiv 0$ modulo p. So u,v,z are zero modulo p. Since (u,v,w,z) is primitive, $p\nmid w$. Since $p\mid v$, we get $p^2\mid u$. Observe that $(u/p^2,v/p,w,z/p)$ is a strong solution modulo m to the system with coefficients (ap^2,c,d).

Conversely, suppose first that (i) the system with coefficients (a,cp^2,d) has a strong solution modulo m. Then it is p-locally solvable by Theorems 2 and 3. Now suppose that (ii) the system with coefficients (ap^2,c,d) has a strong solution modulo m. By Theorems 2 and 3, the system with coefficients (ap^2,c,d) has a primitive solution (u,v,w,z) modulo p^k for any given k. Then (p^2u,pv,w,pz) is a solution modulo p^{k+2} to the original system with coefficients (a,cp^2,d). If it is not primitive, divide the coordinate by the largest common power of p (either p or p^2) to produce a primitive solution. We conclude that, in either case, the system with coefficients (a,cp^2,d) is p-locally solvable. □

Exercise 6. If p is an odd prime then the test for p-local solvability can be made very explicit. For systems (a,c,d) with $p\nmid acd$ we always have p-local solvablility and for systems (a,cp^2,dp) we never have p-local solvability. Show that the systems (a,cp,d) and (a,cp^3,d) are p-locally solvable if and only if ad is a square modulo p. Show that the system (a,c,dp) is p-locally solvable if and only if $-ac^3$ is a fourth power modulo p. Finally, show that the system (a,cp^2,d) is p-locally solvable if and only if ad or cd is a square modulo p.

Relationship with the Quartic. We now relate the systems studied in this paper with the nonhomogeneous quartic equation

$$aX^4+bX^2Y^2+cY^4=dZ^2. \tag{10}$$

The main body of this paper treats the $b=0$ case of the system

$$aU^2+bV^2+cW^2=dZ^2,\qquad UW=V^2, \tag{11}$$

and the appendices consider the general case which is important in the study of elliptic curves. We now show that the solvability of (10) and (11) are equivalent in

many situations. In particular, $\mathbb{Z}$-solvability, $\mathbb{R}$-solvability, and $\mathbb{F}_p$-solvability are covered by the following:

Lemma 11. *Let $a, b, c, d \in R$ where R is an integral domain. Then the system* (11) *has a nontrivial R-solution if and only if* (10) *has a nontrivial R-solution.*

Proof. If $d = 0$ then both (11) and (10) have obvious solutions, so suppose $d \neq 0$.

If (x_0, y_0, z_0) is a nontrivial solution to (10) then $(x_0^2, x_0y_0, y_0^2, z_0)$ is a nontrivial solution to (11).

If (u_0, v_0, w_0, z_0) is a nontrivial solution to (11), then both (u_0, v_0, z_0u_0) and (v_0, w_0, z_0w_0) are solutions to (10). At least one is nontrivial since $d \neq 0$. □

The questions of modulo p^k solvability (for $k > 1$) and p-local solvability are covered by the following. For simplicity we assume $p^2 \nmid d$.

Lemma 12. *Let p be a prime and $k > 1$. Suppose that $a, b, c, d \in \mathbb{Z}$ are such that $p^2 \nmid d$. Then the system* (11) *has a primitive solution modulo p^k if and only if the equation* (10) *has a primitive solution modulo p^k.*

Proof. If (x_0, y_0, z_0) is a primitive solution to (10) modulo p^k then $(x_0^2, x_0y_0, y_0^2, z_0)$ is a primitive solution to (11) modulo p^k.

If (u_0, v_0, w_0, z_0) is a primitive solution to (11) modulo p^k, then (u_0, v_0, z_0u_0) and (v_0, w_0, z_0w_0) are both solution to (10) modulo p^k. Claim: at least one of u_0, v_0 or w_0 must be prime to p. Otherwise, by assumption z_0 is prime to p, and since $dz_0^2 \equiv au_0^2 + bv_0^2 + cw_0^2 \bmod p^k$, it follows that $p^2|d$, a contradiction. With this claim, we see that at least one of the solutions is primitive. □

Appendix A: The p-adic integers and Hensel's lemma

In Section 3 we defined p-local solvability in terms of solvability modulo p^k. As alluded to in the introduction, the usual definition of p-local solvability refers to p-adic solutions rather than solutions modulo p^k. In this appendix we sketch an argument that our definition is equivalent to the p-adic definition. Then we introduce a basic tool, Hensel's Lemma, which is the standard method for finding $\mathbb{Z}_p$-solutions. Both the p-adic integers and Hensel's Lemma will be used in Appendix B where we discuss an important generalization of the systems considered above. This appendix and the next are designed for readers with some familiarity with the p-adic numbers.

We begin with a quick review of the p-adic numbers. A p-adic integer is a sequence $(a_1, a_2, a_3, \ldots)$ with the following properties for each k: (i) $a_k \in \mathbb{Z}/p^k\mathbb{Z}$, and (ii) the image of a_{k+1} under the natural projection $\mathbb{Z}/p^{k+1}\mathbb{Z} \to \mathbb{Z}/p^k\mathbb{Z}$ is equal to a_k. The set $\mathbb{Z}_p$ of such sequences forms an integral domain with addition and multiplication defined componentwise. Its field of fractions is denoted by $\mathbb{Q}_p$. There is a natural injective ring homomorphism $\mathbb{Z} \to \mathbb{Z}_p$ defined by sending a to $(a_1, a_2, \ldots)$ where a_k is the image of a in $\mathbb{Z}/p^k\mathbb{Z}$. Thus we can identify $\mathbb{Z}$ with a subring of $\mathbb{Z}_p$ and $\mathbb{Q}$ with a subfield of $\mathbb{Q}_p$. The multiplicative structure of $\mathbb{Z}_p$ is simple: every nonzero element is uniquely of the form up^m where u is a unit in $\mathbb{Z}_p$. The units of $\mathbb{Z}_p$ are the elements $(a_1, a_2, \ldots)$ such that a_1 is a unit in $\mathbb{Z}/p\mathbb{Z}$. For an introduction to the p-adic numbers, with prerequisites similar to those of the current paper, see [5].

Proposition 4. *For a system of homogeneous equations with coefficients in $\mathbb{Z}$, the following are equivalent:*

(1) *The system has primitive solutions modulo p^k for all k.*
(2) *The system has a nontrivial $\mathbb{Z}_p$-solution.*
(3) *The system has a nontrivial $\mathbb{Q}_p$-solution.*

Proof. The conditions (2) and (3) are equivalent since the system is homogeneous. Suppose (2) holds with nontrivial $\mathbb{Z}_p$-solution $(x_1, \ldots, x_n)$. Let p^λ be the largest power of p dividing all the x_i. By dividing each x_i by p^λ we can assume that at least one coordinate is a unit in $\mathbb{Z}_p$. Write $x_i = (a_{i1}, a_{i2}, \ldots)$. Then, for each k, the n-tuple $(a_{1k}, \ldots, a_{nk})$ yields a solution modulo p^k. Since there is a coordinate x_i that is a $\mathbb{Z}_p$-unit, the corresponding a_{ik} is a $\mathbb{Z}/p^k\mathbb{Z}$-unit. So $(a_{1k}, \ldots, a_{nk})$ is a primitive solution modulo p^k. We conclude that (2) $\Rightarrow$ (1).

Finally suppose that (1) holds. Let n be the number of variables. To produce a $\mathbb{Z}_p$-solution it is sufficient to produce $\mathbf{c_k} = (c_{k1}, \ldots, c_{kn}) \in \mathbb{Z}^n$ for each k such that (i) $\mathbf{c_k}$ is a primitive solution modulo p^k and (ii) $\mathbf{c_{k+1}}$ is congruent (componentwise) to $\mathbf{c_k}$. To facilitate the construction, we also consider the condition (iii) $\mathbf{c_k}$ is infinitely extendable in the following sense: for all $\lambda \geq k$ there is a primitive solution modulo p^λ congruent modulo p^k to $\mathbf{c_k}$.

Let $\mathbf{c_1}$ be a primitive solution modulo p that satisfies (iii). If no such solution exists then either there is no primitive solution modulo p contradicting (1), or there are a finite number of modulo-p-distinct solutions but where each is not infinitely extendible. By choosing λ large enough, we get a modulus p^λ with no primitive solutions, also contradicting (1). Thus $\mathbf{c_1}$ exists. Now suppose $\mathbf{c_u}$ has been selected that satisfies (iii) for $k = u$. Choose $\mathbf{c_{u+1}}$ to be any primitive solution modulo p^{u+1} that reduces modulo p^u to $\mathbf{c_u}$ and for which (iii) holds with $k = u + 1$. Such $\mathbf{c_{u+1}}$ exists: otherwise (iii) would fail for $\mathbf{c_u}$. This construction yields a sequence $\mathbf{c_1}, \mathbf{c_2}, \mathbf{c_3}, \ldots$ satisfying (i), (ii), (iii) for all k. So (1) $\Rightarrow$ (2). □

Hensel's lemma refers to a family of results that allows us to "lift" modulo p solutions to $\mathbb{Z}_p$-solutions. Here is a basic version for polynomials.

Proposition 5. *Let $f \in \mathbb{Z}_p[T]$ be a polynomial with derivative f'. If $t \in \mathbb{Z}_p$ is such that $f(t) \equiv 0 \bmod p$ but $f'(t) \not\equiv 0 \bmod p$, then there is a unique $u \in \mathbb{Z}_p$ such that $f(u) = 0$ and such that $u \equiv t \bmod p$.*

Remark. There are refinements that deal with the case $f'(t) \equiv 0 \bmod p$.

Appendix B: connections to Elliptic Curves

In this appendix we assume some familiarity with elliptic curves defined over $\mathbb{Q}$. Consider the system

$$aU^2 + bV^2 + cW^2 = dZ^2, \qquad UW = V^2 \tag{12}$$

with $a, b, c, d \in \mathbb{Z}$ such that a, c, d, and $b^2 - 4ac$ are nonzero. Up to this point we have concentrated on the simplier case $b = 0$, which is rich enough to yield simple counterexamples to the Hasse principles. In general, (12) defines a nonsingular projective curve of genus 1 given as the intersection of quadric surfaces.[18]

Such genus 1 curves arise naturally in the 2-descent procedure used to find generators and the rank for the group of rational points $E(\mathbb{Q})$ of elliptic curves E.

[18]This curve is a double cover of the projective planar conic $aU^2 + bUW + cW^2 = dZ^2$. By counting ramification points of this cover, and using the Riemann-Hurwitz formula, one can verify that the genus of the curve is indeed one. The curve defined by (12) is an elliptic curve defined over $\mathbb{Q}$ if and only if (12) possesses a nontrivial $\mathbb{Z}$-solution.

The system (12) is adapted to the case where E is defined over $\mathbb{Q}$ and possess at least one $\mathbb{Q}$-rational 2-torsion point, and the question of the existence of nontrivial $\mathbb{Z}$-solutions of (12) plays an important role in the 2-descent procedure.

Another connection between system (12) and elliptic curves occurs when (12) is a counterexample to the Hasse principle. In that case, (12) represents an element of order 2 of the Tate–Shafarevich group $\mathbf{Ш}_G$ of the elliptic curve G defined by the equation $y^2 = x^3 - 2bdx^2 + (b^2 - 4ac)d^2x$. For example, Lind and Reichardt's counterexample, which we studied in the form

$$U^2 - 17W^2 = 2Z^2 \qquad UW = V^2,$$

represents an element of order 2 in $\mathbf{Ш}_G$ where G is defined by $y^2 = x^3 - 2^4 \cdot 17x$ (which can be transformed into the form $y^2 = x^3 - 17x$). The Tate–Shafarevich group is conjecturally finite, and is tied to another important conjecture: the conjecture of Birch and Swinnerton-Dyer.

Much of the study of local solvability considered in the main body of the paper extends to the system (12). For example, we can generalize Corollary 1 as follows:

Theorem 5. *The system* (12) *is p-locally solvable for all primes $p \nmid 2acd(b^2 - 4ac)$.*

We end this appendix with the proof of the above theorem. The idea is to first show that there is a solution modulo p, and then use Hensel's Lemma to derive a $\mathbb{Z}_p$-solution.

One way to prove the existence of solutions modulo p is to use a theorem of F. K. Schmidt (also proved by Châtelet) according to which any smooth curve of genus 1 defined over a finite field $\mathbb{F}_q$ has an $\mathbb{F}_q$-rational point. Similarly, one can appeal to the Riemann hypothesis for curves over a finite field, proved by A. Weil. In this appendix we instead provide an elementary proof of the existence of modulo p solutions.

Lemma 13. *Let p be an odd prime, and consider*

$$aU^2 + bV^2 + cW^2 = dZ^2, \qquad UW = V^2$$

with $a, b, c, d \in \mathbb{F}_p$, and with $acd(b^2 - 4ac) \neq 0$. This system has a nontrivial $\mathbb{F}_p$-solution.

Proof. By multiplying the first equation by d^{-1} we reduce to the case where $d = 1$. We now use the technique of completing the square on $f(X, Y) = aX^2 + bXY + cY^2$. Let $q_1, q_2, q_3 \in \mathbb{F}_p[T]$ be as in Lemma 1 applied to $aX^2 + \left(c - \frac{b^2}{4a}\right) Y^2 = Z^2$. Thus $aq_1^2 + \left(c - \frac{b^2}{4a}\right) q_2^2 = q_3^2$. So, if $q_1' = q_1 - \frac{b}{2a} q_2$ then

$$f(q_1', q_2) = a\left(q_1 - \tfrac{b}{2a} q_2\right)^2 + b\left(q_1 - \tfrac{b}{2a} q_2\right) q_2 + cq_2^2 = aq_1^2 + \left(c - \tfrac{b^2}{4a}\right) q_2^2 = q_3^2.$$

Since q_1 and q_2 are not associates, q_1' is nonzero, and q_1' and q_2 cannot be associates. So, by Lemma 4, there is a $t \in \mathbb{F}_p$ such that $\left(\frac{q_1'(t)}{p}\right) \neq -\left(\frac{q_2(t)}{p}\right)$. So $q_1'(t) q_2(t) = s^2$ for some $s \in \mathbb{F}_p$, and $q_1'(t)$ and $q_2(t)$ are not both 0. In particular, $\big(q_1'(t), s, q_2(t), q_3(t)\big)$ is a nontrivial solution. □

The above gives us modulo p solutions to (12). To use this to produce $\mathbb{Z}_p$-solutions we need a special case of Hensel's lemma:

Lemma 14. *Let p be a prime not dividing $2ac(b^2 - 4ac)$ where $a, b, c \in \mathbb{Z}$. If $f(T) = aT^4 + bT^2 + c$ has a root modulo p, then f has a root in $\mathbb{Z}_p$.*

Proof. Let $t \in \mathbb{Z}$ be such that $f(t) \equiv 0 \bmod p$. Suppose $f'(t) \equiv 0 \bmod p$ where $f' = 4aT^3 + 2bT$. In other words, $-4at^3 \equiv 2bt$ modulo p. Observe that $t \not\equiv 0$ modulo p since $f(0) = c$ and $p \nmid c$. Also p is odd. Thus $-2at^2 \equiv b \bmod p$. So

$$0 \equiv -(4a)at^4 - (4a)bt^2 - (4a)c \equiv -b^2 + 2b^2 - 4ac \equiv b^2 - 4ac \mod p$$

contradicting our assumption. Thus $f'(t) \not\equiv 0 \bmod p$. The result now follows from Hensel's lemma (Proposition 5). □

Proof of Theorem 5. Let (u_0, v_0, w_0, z_0) be a primitive solution to the system (12) modulo p (Lemma 13). If p divides both u_0 and w_0, it must divide v_0 and z_0 as well, contradicting the assumption that the solution is primitive. By symmetry between U and W we can assume that w_0 is prime to p. In particular w_0 is a unit in $\mathbb{Z}_p$.

Let $u = u_0\, w_0^{-1}$, $v = v_0\, w_0^{-1}$, and $z = z_0\, w_0^{-1}$ in $\mathbb{Z}_p$. Then $(u, v, 1, z)$ also solves (12) modulo p. So $u \equiv v^2$, and hence $av^4 + bv^2 + c \equiv dz^2$, modulo p.

We first consider the case where $z \equiv 0$ modulo p. In this case v is a root, modulo p, of the polynomial $f(T) = aT^4 + bT^2 + c$. By Lemma 14, there is a $t \in \mathbb{Z}_p$ such that $f(t) = 0$. Observe that $\big(t^2, t, 1, 0\big)$ is a $\mathbb{Z}_p$-solution to (12).

Now suppose $z \not\equiv 0$ modulo p. Then z is a root, modulo p, of the polynomial $f(T) = d\,T^2 - (av^4 + bv^2 + c)$. Observe that $f'(z) = 2dz \not\equiv 0$ modulo p. By Hensel's lemma (Proposition 5) there is a $t \in \mathbb{Z}_p$ so that $f(t) = 0$. In particular $(v^2, v, 1, t)$ is a $\mathbb{Z}_p$-solution to (12). □

Remark. For more on elliptic curves over $\mathbb{Q}$, consult [1], [16], and [15]. At a more advanced level see [11].

References

[1] J. W. S. Cassels, *Lectures on Elliptic Curves*, Cambridge University Press 1991

[2] J.E. Cremona, D. Rusin, *Efficient solution of rational conics*, Math. Comp. **72** (2003), no. 243, 1417–1441

[3] H. Davenport, *The Higher Arithmetic: An Introduction to the Theory of Numbers*, Dover 1983 (reprint of the original edition of 1952)

[4] C.F. Gauss, *Disquisitiones Arithmeticae*, 1801

[5] F. Q. Gouvêa, *p-adic Numbers*, Springer-Verlag 1997 (second edition)

[6] K. Ireland, M. Rosen, *A Classical Introduction to Modern Number Theory*, Springer-Verlag 1990 (second edition)

[7] J. Kraft, M. Rosen, *Eisenstein reciprocity and n-th power residues*, Amer. Math. Monthly **88** (1981), 269–270

[8] F. Lemmermeyer, *Euler's trick and second 2-descents*, preprint

[9] F. Lemmermeyer, *Reciprocity Laws: From Euler to Eisenstein*, Springer-Verlag 2000

[10] C.-E. Lind, *Untersuchungen über die rationalen Punkte der ebenen kubischen Kurven vom Geschlecht Eins*, Diss. Univ. Uppsala 1940

[11] B. Mazur, *On the passage from local to global in number theory*, Bull. Amer. Math. Soc. (N.S.) **29** (1993), no. 1, 14–50

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

[13] E. Selmer, *The diophantine equation $ax^3 + by^3 + cz^3 = 0$*, Acta Math. **85** (1951), 203–362

[14] J.-P. Serre, *A Course in Arithmetic*, Springer-Verlag 1973

[15] J. H. Silverman, *The Arithmetic of Elliptic Curves*, Springer-Verlag 1986

[16] J. H. Silverman, J. Tate, *Rational Points on Elliptic Curves*, Springer-Verlag 1992

[17] A. Weil, *Number Theory: An Approach through History*, Birkhäuser 1984