COUNTEREXAMPLES TO THE HASSE PRINCIPLE: AN ELEMENTARY INTRODUCTION

W. AITKEN, F. LEMMERMEYER

Abstract. We give an elementary, self-contained exposition concerning counterexamples to the Hasse Principle. Our account, which uses only techniques from standard undergraduate courses in number theory and algebra, focusses 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.

1. Introduction

The solvability of the Diophantine equation

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

was investigated by all the great number theorists from Euler to Gauss.[1] We assume that a, b, and c are non-zero 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 non-trivial $\mathbb{Z}$-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 non-trivial $\mathbb{Z}$-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 (1902) 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 Thm. 1′ Ch. IV of [14]). 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 (Articles 294–300) where another proof of Legendre's theorem is given, and Legendre's proof of quadratic reciprocity is critiqued.

For a proof of Legendre's theorem based on Lagrange's descent see Chapter VII §3 of [5], Chapter 17 §3 of [7], Chapter II §XIV and Chapter IV Appendix I of [18] (which gives historical background including Lagrange's role in the solution to the problem). For more on Legendre's theorem see Exercises 1.8 and 2.36 of [9], and various books on Diophantine equations. Lagrange's descent gives an explicit method for finding a solution if it exists, see Cremona & Rusin [4] for practical improvements on the descent method.

To explain Hasse's result, we will need to fix some terminology. Consider the Diophantine equation

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

where $F \in \mathbb{Z}[X_1, \ldots, X_m]$ is a homogeneous polynomial of degree d (often called a *form* of degree d). The m-tuple $(0, \ldots, 0)$ is a solution, but not an interesting one. The m-tuple $(a_1, \ldots, a_m)$ is called *non-trivial* if at least one a_i is non-zero. We are interested in finding necessary and sufficient conditions for the existence of non-trivial solutions to (2). A non-trivial m-tuple $(a_1, \ldots, a_m) \in \mathbb{Z}^m$ is said to be *primitive* if the greatest common divisor of $a_1, \ldots, a_m$ is 1. Observe that, by homogeneity, if (2) has any non-trivial 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 $F(X_1, \ldots, X_n) \equiv 0$ modulo N.[3]

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

Theorem (Hasse's Theorem: version 1). *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 non-trivial $\mathbb{Z}$-solution if and only if (i) it has a non-trivial $\mathbb{R}$-solution, and (ii) it has a primitive solution modulo N for all positive integers N.*

The Chinese Remainder Theorem allows us to restate this result as follows.

Theorem (Hasse's Theorem: version 2). *If $F \in \mathbb{Z}[X_1, \ldots, X_m]$ is homogeneous of degree 2, then $F(X_1, \ldots, X_m) = 0$ has a non-trivial $\mathbb{Z}$-solution if and only if (i) it has a non-trivial $\mathbb{R}$-solution, and (ii) it has a primitive solution modulo p^k for all primes p and exponents $k \geq 1$.*

In many cases, finding a solution modulo p^k reduces (by Hensel's Lemma, see Appendix A) to finding a solution modulo p. In fact, a natural setting for understanding solutions modulo p^k as k varies is through the *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 nor 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 describe $\mathbb{R}$ as $\mathbb{Q}_\infty$; the fields $\mathbb{Q}_p$ for p a prime or ∞ give all the *completions* of $\mathbb{Q}$ and are called the *local fields*

[3] One can relax the definition of *primitive m-tuple modulo N* to allow any non-trivial m-tuple whose GCD is prime to N. However, any solution to $F(X_1, \ldots, X_n) \equiv 0 \bmod N$ that is primitive modulo N in this sense gives rise to a solution that is primitive according to our definition.

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 non-trivial $\mathbb{Q}$-solution if and only if it has a non-trivial $\mathbb{Q}_p$-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 non-trivial $\mathbb{Z}$-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]

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

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

This cubic obviously has non-trivial $\mathbb{R}$-solutions, and it can be shown (using results described in Appendix C, and Hensel's Lemma described in Appendix A) to have solutions modulo each prime power but *it has no non-trivial $\mathbb{Z}$-solutions.*[5]

What if one sticks to quadratic equations, but allow *systems* of equations? In this paper we will show that this class also fails the Hasse Principle. We will study certain systems of two quadratic equations in four variables, and use completely elementary methods to produce counterexamples to the Hasse Principle. Each such system can be transformed into a quartic non-homogeneous polynomial in three variables. One of our systems transforms into

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

which was the first known counterexample to the Hasse Principle. It was produced by Lind [10] and Reichardt [12] several years before Selmer's. In contrast to Selmer's example, there are proofs, like the one given in Section 7, that (4) has no non-trivial $\mathbb{Z}$-solutions involving only quadratic reciprocity — and there are proofs (see [8]) that

[4] 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 (including $p = \infty$).

[5] Showing the absence of integral solutions is not so easy. 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 $Ш_E$ the elliptic curve $E : X^3 + Y^3 + 60Z^3 = 0$. See [2], [11], and our Appendix D for more on the relationship between counterexamples and the Tate-Shafarevich group.

require even less. The harder part is to give a completely elementary proof that (4) has solutions modulo all primes.[6]

The purpose of this article is to give a self-contained, accessible proof of the existence of counterexamples to the Hasse Principle involving systems of two quadratic equations, counterexamples closely related to those of Lind and Reichart'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.[7] As far as we know, this paper is unique in developing interesting counterexamples to the Hasse Principle in such an elementary manner.[8] Our hope is 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 an very important and active area of current research.[9] As discussed in Appendix D (written for a more advanced reader), 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 non-zero 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 above 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 non-trivial $\mathbb{R}$-solution, then $aX^2 + bY^2 + cZ^2 = 0$ has a non-trivial $\mathbb{Z}$-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.

[6] 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. See Appendix C.

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

[8] 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 2 and 4.

[9] 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.

2. Preliminary Reduction

Selmer's example shows that one cannot extend the Hasse Principle to polynomials of degree greater than two. There is another way, however, that one might try to generalize the Hasse Principle: keep the degree of the polynomials equal to two, but allow *systems* of equations. Does the Hasse Principle hold for all systems

$$F_1(X, Y, Z, W) = 0, \qquad F_2(X, Y, Z, W) = 0 \tag{5}$$

as long as $F_1, F_2 \in \mathbb{Z}[X, Y, Z, W]$ are limited to degree 2? The answer is no, and the main goal of this paper is to give counterexamples.[10]

The Diophantine systems considered in this paper are of the form

$$aU^2 + bV^2 + cW^2 = dZ^2, \qquad UW = V^2 \tag{6}$$

with $a, b, c, d \in \mathbb{Z}$, with d square-free, with a, c, d non-zero, and with $b^2 - 4ac \neq 0$.

The system (6) is closely related to the single (non-homogeneous) equation

$$aX^4 + bX^2Y^2 + cY^4 = dZ^2. \tag{7}$$

In fact, the following lemmas allow us to reduce our study of (6) to (7).

Lemma 1. *The system* (6) *has a non-trivial* $\mathbb{Z}$*-solution if and only if the equation* (7) *has a non-trivial* $\mathbb{Z}$*-solution. Likewise,* (6) *has a non-trivial* $\mathbb{R}$*-solution if and only if* (7) *has a non-trivial* $\mathbb{R}$*-solution.*

Proof. If (x_0, y_0, z_0) is a non-trivial solution to (7) then $(x_0^2, x_0y_0, y_0^2, z_0)$ is a non-trivial solution to (6).

If (u_0, v_0, w_0, z_0) is a non-trivial solution to (6), then then both (u_0, v_0, z_0u_0) and (v_0, w_0, z_0w_0) are solution to (7). At least one of these must be non-trivial. □

Lemma 2. *Let p be a prime, and $k \geq 2$. The system* (6) *has a primitive solution modulo p^k if and only if the equation* (7) *has a primitive solution modulo p^k.*

Proof. If (x_0, y_0, z_0) is a primitive solution to (7) modulo p^k then $(x_0^2, x_0y_0, y_0^2, z_0)$ is a primitive solution to (6) modulo p^k.

If (u_0, v_0, w_0, z_0) is a primitive solution to (6) modulo p^k, then (u_0, v_0, z_0u_0) and (v_0, w_0, z_0w_0) are both solution to (7) 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 $p^2 | d$ contradicting d square-free.

By the above claim, at least one of u_0, v_0 or w_0 has an inverse modulo p^k. For example, if u_0 has inverse u_0^{-1} then $(1, v_0u_0^{-1}, z_0)$ is a primitive solution to (7) modulo p^k. A similar argument shows that if v_0 or w_0 has an inverse modulo p^k then (v_0, w_0, z_0w_0) can be modified to form a primitive solution modulo p^k. □

Remark. If $p \nmid d$, then we can extend the above to $k = 1$.

[10] An important principle of arithmetic geometry is that when classifying a system of Diophantine equations do not look at degree alone, but also look at of other invariants of algebraic geometry such as genus. Selmer's example and system (5) are more similar than they first appear: they both define curves of genus one. Selmer's example is of degree 3 in $\mathbb{P}^2$, but the curve defined by (5) has degree $4 = 2 \cdot 2$ in $\mathbb{P}^3$.

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

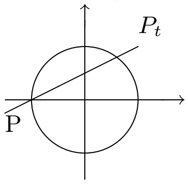

Figure 1. Parametrizing the Unit Circle

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

$$(1-T^2)^2+(2T)^2=(1+T^2)^2. \tag{8}$$

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 non-zero. 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 (8) is displayed in the following lemma as (9).[11]

Lemma 3. *Let F be a field, and let $a,b \in F$ be non-zero. Let $x_0,y_0 \in F$ be such that $ax_0^2+by_0^2=1$. Then in $F[T]$*

$$a(bx_0T^2-2by_0T-ax_0)^2+b(-by_0T^2-2ax_0T+ay_0)^2=(bT^2+a)^2. \tag{9}$$

Let $q_1,q_2,q_3 \in F[T]$ be the polynomials, of degree at most 2, appearing in this equation. So $aq_1^2+bq_2^2=q_3^2$. At least two of q_1,q_2,q_3 have degree exactly 2. If $\operatorname{char} F \neq 2$, each of q_1,q_2,q_3 is non-zero, and no two are associates.[12]

Proof. We can use the parametrization method to find $q_1,q_2,q_3 \in F[T]$, but, once found, verifying $aq_1^2+bq_2^2=q_3^2$ is 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 non-zero, and x_0 and y_0 are not both 0, each of q_1,q_2,q_3 is non-zero. 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 all associates. In other words q_1,q_2 would both be constant multiples of q_3. But either q_1 or q_2 has a non-zero linear term, contradiction. □

[11] In the language of algebraic geometry, a non-singular 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 non-degenerate conic can be brought into the form $ax^2+by^2=1$ with a projective transformation.

[12] Recall that two non-zero polynomials of $F[t]$ are *associates* if one is a constant multiple of the other.

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 finite fields, proving the existence of such a point is easy.[13]

Lemma 4. *Let a and b be non-zero element 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 $\left(\frac{f(t)}{p}\right) = -1$ 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. According to Weil ([18] Chapter III §XI) 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). For that theorem, one uses the solvability of the congruence $x^2 + y^2 + 1 \equiv 0 \bmod p$.

Remark. As we have seen, methods for parameterizing 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 •, and the unit circle $x^2 + y^2 = 1$ consisting of 8 points, denoted by •. 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?

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 $1 \leq x \leq 6$ are exterior points since they lie on the tangent at $(1, 0)$.

4. The equation $aX^4 + bY^4 = Z^2$ over finite fields

Let p be an odd prime. Our parametrization for the conic $ax^2 + by^2 = 1$ gives a tool for solving $aX^4 + bY^4 = Z^2$ in $\mathbb{F}_p$. For lifting at least one solution from the conic to the quartic, we need another ingredient.[14]

Proposition 1. *Let $f, g \in \mathbb{F}_p[X]$ be non-zero 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.*

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 $f^{(p-1)/2} - g^{(p-1)/2}$.

[13] The following proof extends to any finite field F since $F^\times$ is cyclic (and for F of even order the result is trivial: every element is a square).

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

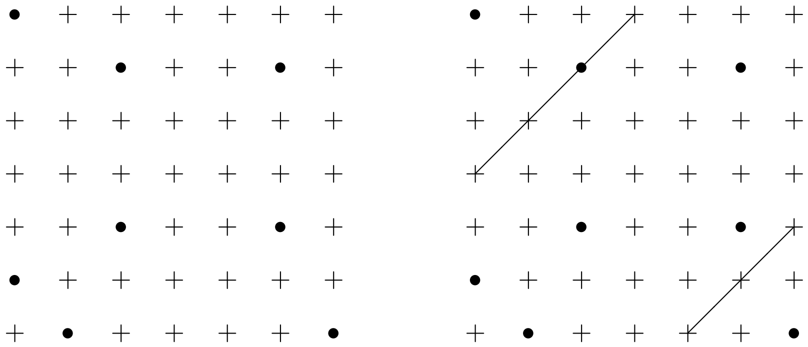

FIGURE 2. The Unit Circle over $\mathbb{F}_7$, and its tangent at $(2,5)$

So $f^{(p-1)/2} - g^{(p-1)/2}$ is the zero polynomial: otherwise it would be a polynomial of degree at most $p-1$ with p roots, which is impossible over fields. But since $\mathbb{F}_p[X]$ is a unique factorization domain, $f^{(p-1)/2} = g^{(p-1)/2}$ implies that f and g are associates.

If $\big(\frac{f(t)}{p}\big) = -\big(\frac{g(t)}{p}\big)$ for all $t \in \mathbb{F}_p$, pick a non-square $r \in \mathbb{F}_q^\times$. Observe that $\big(\frac{f(t)}{p}\big) = \big(\frac{rg(t)}{p}\big)$ for all $t \in \mathbb{F}_p$, which is the previous case. □

Our experience in Section 2 tells us that solving $aX^4 + bY^4 = Z^2$ is related to solving the system $aX^2 + bY^2 = Z^2$ and $XY = S^2$. We can parameterize the first of these equations, leaving the second to be solved. This motivates the following.

Theorem 1. *Let p be an odd prime, and let $a, b \in \mathbb{F}_p$ be non-zero. Then the equation $aX^4 + bY^4 = Z^2$ has a non-trivial $\mathbb{F}_p$-solution.*

Proof. Let $q_1, q_2, q_3 \in \mathbb{F}_p[T]$ be as in Lemma 3. So $aq_1^2 + bq_2^2 = q_3^2$. (The existence of suitable $x_0, y_0 \in \mathbb{F}_q$ is given by Lemma 4.)

By Proposition 1 and that fact that q_1 and q_2 are not associates, there is a $t \in \mathbb{F}_p$ such that $\big(\frac{q_1(t)}{p}\big) \neq -\big(\frac{q_2(t)}{p}\big)$. So $q_1(t)$ and $q_2(t)$ are not both zero and $\big(\frac{q_1(t)q_2(t)}{p}\big) \neq -1$. Thus $q_1(t)q_2(t) = s^2$ for some $s \in \mathbb{F}_p$.

Suppose that $q_1(t) \neq 0$. Then $\big(q_1(t), s, q_1(t)q_3(t)\big)$ is a non-trivial solution to $aX^4 + bY^4 = Z^2$. Likewise, if $q_2(t) \neq 0$ then $\big(s, q_2(t), q_2(t)q_3(t)\big)$ is a solution. □

5. Powers modulo p^k

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

Proposition 2. *Let p be a prime, and let N and $r > 0$ be integers such that $p \nmid rN$. If N is a rth power modulo p, then N is an rth power modulo p^k for all $k \geq 1$.*

Proof. (By 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,

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

□

An application of this is the following.

Proposition 3. *Let p be an odd prime not dividing $a, c, d \in \mathbb{Z}$. Then, for all $k \geq 1$, the equation $aX^4 + cY^4 = dZ^2$ has a primitive solution (x_k, y_k, z_k) modulo p^k.*

Proof. Since $(p^k, d) = 1$, there is an inverse $d^{-1} \in \mathbb{Z}$ for d modulo p^k. By Theorem 1, $d^{-1}aX^4 + d^{-1}cY^4 \equiv Z^2 \bmod p$ has a solution (x_1, y_1, z_1) with $x_1, y_1, z_1 \in \mathbb{Z}$ not all divisible by p.

If $p \nmid z_1$ then let $N = d^{-1}(ax_1^4 + cy_1^4)$. By Proposition 2, $N \equiv n^2 \bmod p^k$ for some $n \in \mathbb{Z}$, and (x_1, y_1, n) is a solution modulo p^k. If $x_1 \not\equiv 0 \bmod p$, then let x_1^{-1} be an inverse to x_1 modulo p^k. Then $(1, y_1 x_1^{-1}, n x_1^{-2})$ is a primitive solution modulo p^k. If $x_1 \equiv 0 \bmod p$, then take $(x_1 y_1^{-1}, 1, n y_1^{-2})$ instead.

If $p \mid z_1$, let c^{-1} be an inverse for c modulo p^k. From $ax_1^4 + cy_1^4 \equiv 0 \bmod p$, we get that $N = -ac^{-1}$ is a non-zero fourth power modulo p. By Proposition 2, there is an n such that $N \equiv n^4 \bmod p^k$, and $(1, n, 0)$ is a primitive solution modulo p^k. □

For $p = 2$ the situation for fourth powers is a little more delicate.

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

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

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

□

6. Solutions modulo p^k

Proposition 3, together with Lemma 2, immediately gives us the following.[15]

Theorem 2. *Suppose a, c and d are non-zero integers where d is square-free. Then the system*

$$aU^4 + cW^4 = dZ^2 \qquad UW = V^2$$

has a primitive solution modulo p^k for all $p \nmid 2acd$ and all $k \geq 1$.

We now have all the ingredients necessary to produce systems that have solutions modulo every prime power. Consider the system

$$U^2 - qW^2 = dZ^2, \qquad UW = V^2 \tag{10}$$

where

(1) q is a prime such that $q \equiv 1 \bmod 16$,
(2) d is a square-free,
(3) d is a non-zero square modulo q, and
(4) q is a fourth power modulo p for every odd p dividing d.

Proposition 5. *The system (10) has primitive solutions modulo p^k for every primes p and exponent $k \geq 1$. In addition, it has real solutions.*

Proof. The existence of a real solution is obvious: consider $(q^{1/2}, q^{1/4}, 1, 0)$.

By the above theorem, we only need to consider primes p not dividing $2qd$.

By Lemma 2, to find primitive solutions modulo p^k with $k \geq 2$ it suffices to find primitive solutions modulo p^k to the equation $X^4 - qY^4 = dZ^2$.

[15] This theorem will be generalized as Theorem 5 in Appendix B.

Suppose $p = q$. Since d is a non-zero square modulo q, Proposition 2 implies that $d \equiv n^2 \bmod q^k$ for some $n \in \mathbb{Z}$, and $(1, 0, n^{-1})$ is a solution to $X^4 - qY^4 = dZ^2$ modulo q^k (where n^{-1} is an inverse for n modulo q^k).

Suppose $p \mid d$ where p is odd. Then, by Proposition 2, $q \equiv n^4 \bmod p^k$ for some $n \in \mathbb{Z}$, and $(n, 1, 0)$ is a solution to $X^4 - qY^4 = dZ^2$ modulo p^k.

Suppose $p = 2$. Proposition 4 guarantees the existence of an $n \in \mathbb{Z}$ with $q \equiv n^4 \bmod 2^k$, and $(n, 1, 0)$ is a solution to $X^4 - qY^4 = dZ^2$ modulo 2^k. □

7. Counterexamples to the Hasse Principle

Consider the Diophantine equation $X^4 - qY^4 = dZ^2$ where $q \equiv 1 \bmod 8$ is a prime and where d is square-free and prime to q. We begin by a developing a necessary condition for this equation to have a non-trivial $\mathbb{Z}$-solution. By forming examples where this necessary condition fails, we produce counterexamples to the Hasse Principle.

First observe that if $X^4 - qY^4 = dZ^2$ has a non-trivial $\mathbb{Z}$-solution (x_0, y_0, z_0) then it has a primitive solution (x_1, y_1, z_1) with x_1, y_1, and z_1 pairwise relatively prime. (To see this, suppose a prime p divides two of x_0, y_0, z_0. Then p must divide x_0. Also, p^2 must divide qy_0^4. Since q is prime, p divides y_0. Thus p^4 divides dz_0^2. Since d is square-free, p^2 must divide z_0. With $x_0/p, y, x_0/p$, and z_0/p^2, we get a smaller solution. Continue this process until the desired (x_1, y_1, z_1) is produced.)

Let (x_1, y_1, z_1) be as above, and let p be an odd prime dividing z_1. Since x_1 and y_1 are prime to z_1 and hence to p, the congruence $x_1^4 - qy_1^4 \equiv 0 \bmod p$, implies that $(\frac{q}{p}) = 1$. By quadratic reciprocity, $(\frac{p}{q}) = 1$ for all such p. Now $q \equiv 1 \bmod 8$, so -1 and 2 are quadratic residues modulo q. Thus z_1 is the product of quadratic residues: $(\frac{z_1}{q}) = 1$. The congruence $d \equiv z_1^{-2} x_1^4 \bmod q$ now implies that d is a fourth power modulo q. To summarize:

Theorem 3. *Let $d \in \mathbb{Z}$ be square-free. Let $q \equiv 1 \bmod 8$ be a prime not dividing d. If $X^4 - qY^4 = dZ^2$ has a nontrivial $\mathbb{Z}$-solution, then d is a fourth power modulo q.*

So to get counterexamples we need to require that d not be a fourth power modulo q. This, combined with the requirements of the previous section gives us the following class of examples. Consider the system of homogeneous Diophantine equations

$$U^2 - qW^2 = dZ^2, \qquad UW = V^2 \tag{11}$$

where

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

Proposition 5, Theorem 3, and Lemma 1 together gives us our main result.

Theorem 4. *The system* (11) *fails the Hasse Principle.*

We end with a few specific examples of (11).

Example 1. 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 $2 \in (\mathbb{F}_{17}^\times)^2$ but $2 \notin (\mathbb{F}_{17}^\times)^4$. This example is often stated in terms of the equivalent Diophantine problem $X^4 - 17Y^4 = 2Z^2$.

Example 2. 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. Of course, $(\frac{2}{q}) = 1$, so

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

gives a counterexample to the Hasse Principle.[16]

Example 3. For an example where $d \neq 2$, consider

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

Appendix A: Hensel's Lemma and the p-adic integers

Hensel's Lemma refers to a family of results that let us modify or "lift" solutions modulo p^k to solutions modulo p^{k+1}. Hensel's Lemma is closely connected to Newton's method from calculus. Here is a basic version.

Proposition 6 (Hensel's Lemma)**.** *Let $f \in \mathbb{Z}[T]$ be a polynomial with derivative f'. If $t_k \in \mathbb{Z}$ is such that $f(t_k) \equiv 0 \bmod p^k$ but $f'(t_k) \not\equiv 0 \bmod p$, then there is a unique $t_{k+1} \in \mathbb{Z}$ such that $t_{k+1} \equiv t_k \bmod p^k$ and $f(t_{k+1}) \equiv 0 \bmod p^{k+1}$.*

Proof. We have $f(t_k) = ap^k$ for some integer a, and if $p \mid a$ we are done: just set $t_{k+1} = t_k$. If $p \nmid a$, we can try to modify t_k modulo p^k: put $t_{k+1} = t_k + xp^k$. Our goal is to determine x in such a way that $f(t_{k+1}) \equiv 0 \bmod p^{k+1}$.

By the following Lemma and Corollary,

$$f(t_k + xp^k) \equiv f(t_k) + f'(t_k)xp^k \equiv (a + xf'(t_k))p^k \bmod p^{k+1}.$$

There is a unique x that makes the right hand side vanish since $p \nmid f'(t_k)$. □

Remark. Stronger forms of Hensel's Lemma address the case where $f'(t_k) \equiv 0$ modulo p

The following makes precise, in our context, the idea that $f(c) + f'(c)T$ approximates $f(T + c)$ to first order.

Lemma 5. *Given a polynomial $f \in \mathbb{Z}[T]$ and a constant $c \in \mathbb{Z}$, there is a polynomial $g \in \mathbb{Z}[T]$ such that $f(T + c) = f(c) + f'(c)T + g(T)T^2$.*

Proof. Show that T^2 divides $f(T + c) - f(c) - f'(c)T$, first for monomials $f = T^n$ using the binomial expansion, and then for all polynomials using linearity. □

Corollary 1. *Given a polynomial $f \in \mathbb{Z}[T]$, constants $c, d \in \mathbb{Z}$, and a prime p, then $f(dp^k + c) \equiv f(c) + f'(c)dp^k \bmod p^{k+1}$ for all $k \geq 1$.*

Hensel's Lemma motivates the study of p-adic numbers. Let p be a prime. A *p-adic integer* is a sequence $(a_1, a_2, a_3, \ldots)$ such that for each k, (i) $a_k \in \mathbb{Z}/p^k\mathbb{Z}$, (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 p-adic integers is a ring when addition and multiplication are defined componentwise. In fact, $\mathbb{Z}_p$ is an integral domain, and its field of fractions

[16] Actually, we need only assume $q \equiv 1 \bmod 8$, as can easily be seen by looking at the $p = 2$ case in the proof of Proposition 5: if $d = 2$, then there is a solution with $Y = 1$ and $Z = 2$. 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 Chebotarev Density Theorem to $\mathrm{Gal}\big(\mathbb{Q}(2^{1/4}, i)/\mathbb{Q}\big)$, a dihedral group of order 8.

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 ring $\mathbb{Z}_p$ has unique factorization: in fact every non-zero 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 $\mathbb{Z}/p\mathbb{Z}$. The ring $\mathbb{Z}_p$ and field $\mathbb{Q}_p$ can be made into a complete metric spaces with some rather interesting properties. For an introduction to the p-adic numbers, with prerequisites similar to those of the current paper, see [6].

An example might help give a sense for how the p-adic numbers behave. Consider the unit circle over $\mathbb{Z}/3\mathbb{Z}$. It has four points, namely $(\pm 1, 0)$, $(0, \pm 1)$. Over the ring $\mathbb{Z}/9\mathbb{Z}$, the unit circle has already 12 points: each point from $\mathbb{Z}/3\mathbb{Z}$ lifts to three distinct points modulo 9 (this can be seen using Hensel's Lemma). Similarly, each point on the unit circle over $\mathbb{Z}/9\mathbb{Z}$ lifts to three points over $\mathbb{Z}/27\mathbb{Z}$, so that $x^2 + y^2 \equiv 1 \bmod 27$ has 36 different solutions. Using induction, we can prove that this process continues forever. This gives us a big tree of solutions modulo $\mathbb{Z}/3^k\mathbb{Z}$; a point on the unit circle with coordinates in $\mathbb{Z}_3$ is by definition any branch in this tree. One such point (x, y), given by the branch

$$(1,0) \;\text{——}\; (1,3) \;\text{——}\; (10,12) \;\text{——}\; \cdots,$$

has coordinates with 3-adic expansion $x = 1 + 0 \cdot 3 + 1 \cdot 9 + \ldots$ and $y = 0 + 1 \cdot 3 + 1 \cdot 9 + \ldots$.

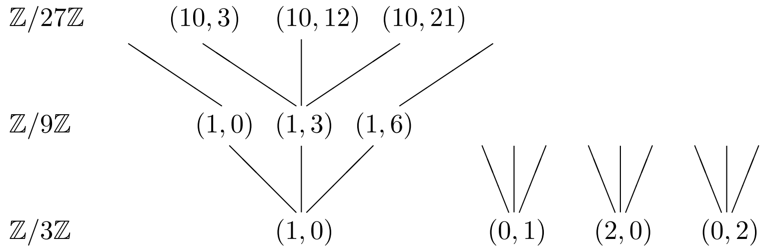

Figure 3. The Unit Circle over $\mathbb{Z}_3$

A p-adic solution to a polynomial equation $f(X_1, \ldots, X_m) = 0$, where f has integer coefficients, gives simultaneously a solution to $f(X_1, \ldots, X_m) \equiv 0 \bmod p^k$ for every exponent $k \geq 1$, and these solutions are "coherent": the solution modulo p^{k+1} reduces modulo p^k to the solution modulo p^k.

In this paper, for example in Proposition 5, we discussed having solutions modulo p^k for all k, but ignored the coherence among the solutions. The following shows that we always get a coherent sequence of solutions given the existence of a possibly non-coherent sequence of solutions. For convenience it is stated for a single polynomial in $\mathbb{Z}[X, Y, Z]$, but of course it generalizes easily to m variables, to systems, and to polynomials with coefficients in $\mathbb{Z}_p$.

Lemma 6. *Let $f \in \mathbb{Z}[X, Y, Z]$ be a polynomial and p a prime such that the equation $f(X, Y, Z) = 0$ has a primitive solution modulo p^k for every $k \geq 1$. Then there are p-adic integers $x, y, z \in \mathbb{Z}_p$, one of which is a unit, such that $f(x, y, z) = 0$.*

Proof. We say that two triples (a_1, b_1, c_1) and (a_2, b_2, c_2) in $\mathbb{Z}^3$ *agree modulo* p^k if

$$a_1 \equiv a_2 \bmod p^k, \quad b_1 \equiv b_2 \bmod p^k, \quad \text{and} \quad c_1 \equiv c_2 \bmod p^k.$$

Let (x_1, y_1, z_1), (x_2, y_2, z_2), (x_3, y_3, z_3), $\ldots$ be a sequence of primitive solutions where (x_k, y_k, z_k) is a solution to $f(X, Y, Z) = 0$ modulo p^k. Our job is to form a coherent sequence out of this sequence. Suppose we have succeeded up to n. More precisely, let n be such that for all $k < n$ a choice of primitive solution (x'_k, y'_k, z'_k) modulo p^k has been made in such a way that (i) (x'_k, y'_k, z'_k) agrees modulo p^k with an infinite number of (x_l, y_l, z_l) from the original sequence, and (ii) if $k > 1$ then (x'_k, y'_k, z'_k) agrees modulo p^{k-1} with $(x'_{k-1}, y'_{k-1}, z'_{k-1})$. We must find a (x'_n, y'_n, z'_n) such that the above properties (i) and (ii) holds also for the case $k = n$.

To that end, partition the triples (x_l, y_l, z_l) from the original sequence into classes, where two triples are in the same class if and only if they agree modulo p^n. If $n > 1$ then remove all triples except those that agree modulo p^{n-1} with $(x'_{n-1}, y'_{n-1}, z'_{n-1})$. There are an infinite number of such triples, so at least one class will be infinite. Let (x'_n, y'_n, z'_n) be any member from such a class.

Let $x = (a_1, a_2, \ldots)$ where a_k is the image of x'_k in $\mathbb{Z}/p^k\mathbb{Z}$. Define y and z in a similar manner. □

Using the above coherence results, Proposition 5 can be rephrased in terms of the existence of solutions in $\mathbb{Z}_p$ and $\mathbb{R}$, so called *local solutions.*

A $\mathbb{Z}_p$ version of Hensel's Lemma follows from the earlier version.

Proposition 7 (Hensel's Lemma: version 2)**.** *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. As in the first version of Hensel's lemma, there are refinements that deal with the case $f'(t) \equiv 0 \bmod p$.

Appendix B: Extending Theorem 2

Consider again the system

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

with $a, b, c, d \in \mathbb{Z}$, with d square-free, and with $acd(b^2 - 4ac) \neq 0$. For simplicity, we concentrated on the case $b = 0$ in the above exposition. The general case, however, is important in the study of elliptic curves (see Appendix D). So it is worthwhile to have an elementary proof of the following.

Theorem 5. *The system* (12) *has a primitive solution modulo p^k for all primes $p \nmid 2acd(b^2 - 4ac)$ and all exponents $k \geq 1$.*

By Lemma 2, proving this theorem reduces to proving Proposition 8 stated below (a generalization of Proposition 3). The remainder of this appendix will be devoted to an elementary proof of Proposition 8. For this we need a generalization of Theorem 1.[17]

Theorem 6. *Let p be an odd prime, and let $a, b, c \in \mathbb{F}_p$ be such that $a \neq 0$ and $b^2 - 4ac \neq 0$. Then the equation $aX^4 + bX^2Y^2 + cY^4 = Z^2$ has a non-trivial $\mathbb{F}_p$-solution.*

[17] Theorem 6 and its proof extend easily to finite fields of odd order.

Proof. We 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 3 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 non-zero, and q_1' and q_2 cannot be associates. So, by Proposition 1, 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.

Suppose that $q_1'(t) \neq 0$. Then $\big(q_1'(t), s, q_1'(t) q_3(t)\big)$ is a non-trivial solution to $f(X^2, Y^2) = Z^2$. If $q_2(t) \neq 0$ then $\big(s, q_2(t), q_2(t) q_3(t)\big)$ is a non-trivial solution. □

Another ingredient for the proof of Proposition 8 is the following

Lemma 7. *Let p be a prime not dividing $2ac(b^2 - 4ac)$ where $a, b, c \in \mathbb{Z}$. If $f = aT^4 + bT^2 + c$ has a root modulo p, then f has a root modulo p^k for all $k \geq 1$.*

Proof. Let $t \in \mathbb{Z}$ be such that $f(t) \equiv 0 \bmod p$. Suppose $f'(t) \equiv 0 \bmod p$ where $f' = 4aT^3 + 2bT$. Since $p \nmid c$, we know that $t \not\equiv 0 \bmod p$. Thus $-2at^2 \equiv b \bmod p$. So

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

contradicting our assumption. Thus $f'(t) \not\equiv 0 \bmod p$. The result now follows from Hensel's Lemma (Proposition 6). □

Proposition 8. *Let $a, b, c, d \in \mathbb{Z}$. Let p be a prime not dividing $2acd(b^2 - 4ac)$. Then, for all $k \geq 1$, the equation $aX^4 + bX^2Y^2 + cY^4 = dZ^2$ has a primitive solution (x_k, y_k, z_k) modulo p^k.*

Proof. Let $f = ad^{-1}X^2 + bd^{-1}XY + cd^{-1}Y^2$ where d^{-1} is an inverse of d modulo p^k. By Theorem 6, the equation $f(X^2, Y^2) = Z^2$ has a non-trivial solution (x_1, y_1, z_1) modulo p.

If $z_1 \not\equiv 0 \bmod p$ then, by Proposition 2, $f(x_1^2, y_1^2) \equiv n^2 \bmod p^k$ for some $n \in \mathbb{Z}$, and (x_1, y_1, n) is a solution modulo p^k. If $x_1 \not\equiv 0 \bmod p$, then let x_1^{-1} be an inverse of x_1 modulo p^k. Then $(1, y_1 x_1^{-1}, n x_1^{-2})$ is a primitive solution modulo p^k. If $x_1 \equiv 0 \bmod p$, then take $(x_1 y_1^{-1}, 1, n y_1^{-2})$ instead.

If $z_1 \equiv 0 \bmod p$, then $x_1 y_1^{-1}$ is root modulo p of the polynomial $f(T^2, 1) \in \mathbb{Z}[T]$. By Lemma 7, there is a $t \in \mathbb{Z}$ such that $f(t^2, 1) \equiv 0 \bmod p^k$. Thus $(t, 1, 0)$ is the desired solution. □

Appendix C: Curves over Finite Fields

The main purpose for this paper is to give an accessible account of a class of counter-examples to the Hasse Principle. An innovation here is proving significant cases of local solvability without recourse to more sophisticated results such as the Riemann hypothesis for curves over a finite field. The following remarks are for the benefit of the reader who wishes to see how the results of this paper connect to the theory of algebraic curves over finite fields.

Lemma 4 is a very special case of the Chevalley–Warning Theorem.[18]

[18] See [1, p. 6] or [14, Chap. 1, § 2] for textbook versions, or [3] and [17] for the original publications. Some sources call it the theorem of Chevalley-Waring, confusing Ewald Warning (1910 – 1999) with the more famous Edward Waring (1736 – 1798).

Theorem 1 and its generalization Theorem 6 are a consequence of 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. Schmidt's proof used zeta functions of function fields and the theorem of Riemann-Roch. To see the implication, first show that if a, b, c, d are in a field F with $\operatorname{char} F \neq 2$ then

$$aU^2 + bV^2 + cW^2 = dZ^2, \qquad UW = V^2 \tag{13}$$

defines a non-singular curve C of genus 1 over F whenever a, c, d, and $b^2 - 4ac$ are non-zero.[19] So C has an $\mathbb{F}_p$-point due to Schmidt's Theorem. By a reduction similar to that given in Section 2, Theorem 6 and its special case Theorem 1 follow.

F. K. Schmidt's Theorem in turn follows from the Riemann hypothesis for curves over a finite field, proved by A. Weil, according to which the number N_q of $\mathbb{F}_q$-rational points on a smooth projective curve of genus g defined over $\mathbb{F}_q$ satisfies $|N_q - (q+1)| \leq 2g\sqrt{q}$. In particular, $N_q \geq 1$ if $g = 1$.

The Weil bound for the curve C defined by (13) can be used to show the existence of W-affine points (that is, points with $W \neq 0$). If $q > 5$ the Weil bound gives $N_q > 2$. Thus C has at least one point of the form $(u, v, 1, z)$. In particular, the affine equation $aV^4 + bV^2 + c = dZ^2$ has an $\mathbb{F}_q$-solution if $a, b, c, d \in \mathbb{F}_q$ and $30acd(b^2 - 4ac) \neq 0$. For $q = 3, 5$ there are not always W-affine $\mathbb{F}_q$-points: for example, $q = 3, a = d = 1, b = c = 2$, or $q = 5, a = d = 1, b = 0, c = 2$.

Appendix D: Relationship with Elliptic Curves

The Diophantine systems considered above are of the form

$$aU^2 + bV^2 + cW^2 = dZ^2, \qquad UW = V^2 \tag{14}$$

with $a, b, c, d \in \mathbb{Z}$. When a, c, d, and $b^2 - 4ac$ are non-zero, these equations define non-singular projective curves of genus 1 given as intersections of quadric surfaces. We can easily reduce to the case $d = 1$, so we do so for much of this appendix.

These genus 1 curves arise naturally in the two-descent procedure used to find generators and the rank for the group of rational points $E(\mathbb{Q})$ of elliptic curves E.[20] The $\mathbb{Q}$-solvability of (14) plays an important role in this two-descent procedure. In addition, when (14) is a counter-example to the Hasse Principle, it represents an element of order two of the Tate-Shafarevich group Ш_G of a certain elliptic curve G. The Tate-Shafarevich group is conjecturally finite, and is tied to another important conjecture: the Birch, Swinnerton-Dyer conjecture.

In this appendix we give a short concrete introduction to some of these ideas directed to a reader with some familiarity with elliptic and algebraic curves.[21] The elliptic curves associated with (14) are defined over $\mathbb{Q}$ and have at least one rational 2-torsion point. Such elliptic curves can be put into the form

$$E : y^2 = x(x^2 + bx + c) \qquad b, c \in \mathbb{Z} \qquad c \neq 0,\ b^2 - 4c \neq 0 \tag{15}$$

or $Y^2S = X(X^2 + bXS + cS^2)$ in homogeneous coordinates. The point of infinity is the identity element, and $(0, 0)$ as a 2-torsion point. The other 2-torsion points, points $(x_0, 0)$ where x_0 is a root of $x^2 + bx + c$, may or may not be rational.

[19] For example, apply the Riemann-Hurwitz formula to the double cover $C \to D$ defined by $(u, v, w, z) \mapsto (u, v, w)$ where D is the genus 0 plane conic defined by $UW = V^2$.

[20] By the Mordell-Weil theorem, $E(\mathbb{Q})$ is a finitely-generated abelian group.

[21] See [2], [16], and [15] for more information.

Partitioning points on an Elliptic Curve. Let E be defined by (15). There is a natural way to partition the points of $E(\mathbb{Q})$ based on the square-free part of the x-coordinate. This turns out to be a finite partition corresponding to cosets of a certain subgroup of $E(\mathbb{Q})$. Curves of the form (14) arise naturally when parameterizing points in a fixed coset. As we will see, the number of such cosets is closely related to the rank of $E(\mathbb{Q})$.

To see how (14) arises from such parameterization, we define the *square-free type* of $(x_0, y_0) \in E(\mathbb{Q})$. If $x_0 \neq 0$ this invariant is defined to be the unique square-free integer γ such that γx_0 is a square in $\mathbb{Q}^\times$. For the point at infinity this invariant is defined as $\gamma = 1$, and for $(0,0)$ this invariant is defined as the unique square-free divisor γ of c such that γc (and c/γ) is a square. We will see later that the square-free type of each point is a (possibly negative) divisor of c.

The square-free type is an invariant compatible with the group law on $E(\mathbb{Q})$. To see this, consider the line $y = tx + r$ with $r \neq 0$ that intersects E in three $\mathbb{Q}$-rational points. Observe that the x-coordinates of the three points are the roots of a monic cubic with constant term $-r^2$. Thus the the product of the x-coordinates of the three points is r^2. So, generically, multiplication of square-free types (modulo squares) is compatible with the group law on $E(\mathbb{Q})$. A separate argument for lines of the form $x = r$ and $y = tx$ gives compatibility in all cases.[22] This gives us the following result:

$$(x_0, y_0) \mapsto [\gamma] \quad \textit{is a homomorphism} \quad E(\mathbb{Q}) \to \mathbb{Q}^\times / \left(\mathbb{Q}^\times\right)^2$$

where $[\gamma]$ is the class of the square-free type of (x_0, y_0). Of course, when $x_0 \neq 0$ this map can also be described more simply as $(x_0, y_0) \mapsto [x_0]$.

Consider first the case $x_0 \neq 0$ where $(x_0, y_0) \in E(\mathbb{Q})$. Let γ be its square-free type. Since γx_0 is a square, (15) tells us that $\gamma(x_0^2 + bx_0 + c)$ is also a square in $\mathbb{Q}^\times$. In particular, there are $v_0, z_0 \in \mathbb{Q}$ such that $x_0 = \gamma v_0^2$ and $x_0^2 + bx_0 + c = \gamma z_0^2$. Choose the signs of v_0 and z_0 so that $y_0 = \gamma v_0 z_0$. So if $u_0 = x_0/\gamma$ and $w_0 = 1$, then (u_0, v_0, w_0, z_0) is a non-trivial $\mathbb{Q}$-solution to

$$\gamma U^2 + bV^2 + \gamma' W^2 = Z^2, \qquad UW = V^2. \tag{16}$$

where $\gamma' = c/\gamma$. As we will see, γ' is an integer, so (16) is a case of (14).

To establish that γ divides c and that γ' is indeed an integer, multiply the above solution by a constant so that the result (u_1, v_1, w_1, z_1) is a primitive solution. Observe that $\gamma^2 u_1^2 + \gamma b v_1^2 + c w_1^2 = \gamma z_1^2$. Let p be a prime divisor of γ. Observe that $c w_1^2$ must be divisible by p. Suppose p divides w_1. So p must divide v_1 since $u_1 w_1 = v_1^2$. Thus $p^2 \mid \gamma z_1^2$. Since γ is square-free, $p \mid z_1$. Since the solution is primitive, $p \nmid u_1$. But $u_1 w_1 = v_1^2$, so $p^2 \mid w_1$. Thus $\gamma^2 u_1^2$ is divisible by p^3 contradicting that γ is square-free and u_1 is prime to p. This contradiction implies that $p \nmid w_1$, so $p \mid c$. Since γ is square-free, we conclude that $\gamma \mid c$.

In particular, *the square-free type of a point divides c, and the image of the homomorphism* $E(\mathbb{Q}) \to \mathbb{Q}^\times / (\mathbb{Q}^\times)^2$ *is finite.*

When $x_0 \neq 0$ we saw that (16) has a solution for the associated γ. For the point at infinity, whose type is $\gamma = 1$, (16) has the solution $(1,0,0,1)$. For the point $(0,0)$, we have that $\gamma' = c/\gamma$ is a square. In this case, there is a solution of the form $(0,0,1,z_0)$. Thus we see that *if there are points of square-free type* γ*, then the associated system (16) has a non-trivial* $\mathbb{Q}$*-solution.*

[22] These special cases motivate our definition of square-free type for infinity and $(0,0)$.

The converse is true as well. To see this let Q_γ be the projective curve defined by (16). Observe that

$$X = \gamma V^2, \quad Y = \gamma V Z, \quad S = W^2$$

defines a algebraic map $Q_\gamma \to E$, (but use $X = \gamma U^2 V, \quad Y = \gamma U^2 Z, \quad S = V^3$ if $W = 0$). Also observe that the image of $Q_\gamma(\mathbb{Q}) \to E(\mathbb{Q})$ consists of points of type γ (even in the special case of points with $V = 0$). So, *there are points of square-free type γ if and only if (16) has a non-trivial $\mathbb{Q}$-solution. More specifically, the set of points of square-free type γ consists of the image of the map $Q_\gamma(\mathbb{Q}) \to E(\mathbb{Q})$*

In particular, the image of $Q_1(\mathbb{Q})$ is the kernel of $E(\mathbb{Q}) \to \mathbb{Q}^\times / (\mathbb{Q}^\times)^2$, and so the image of $Q_1(\mathbb{Q})$ is a subgroup of $E(\mathbb{Q})$. The points of a fixed square-free type is a coset for this subgroup, and finding the number of cosets, i.e., the size of the image $E(\mathbb{Q}) \to \mathbb{Q}^\times / (\mathbb{Q}^\times)^2$, reduces to determining which systems (16) have non-trivial $\mathbb{Q}$-solutions for each γ dividing c.

A 2-Isogeny. Let E be the elliptic curve defined above by (15) and let E' be the elliptic curve defined by $y^2 = x\big(x^2 - 2bx + (b^2 - 4c)\big)$. The partition of points on the elliptic curve E given above is closely related to an isogeny $E' \to E$ of degree 2.[23] This isogeny will play a key role in determining the rank of $E(\mathbb{Q})$. To define this isogeny, we need to prove the following lemma of independent interest: it asserts that any elliptic curve of the form (15) is a special case of the type of curves (14) considered in this paper.

Lemma 8. *The elliptic curve defined by (15) is isomorphic, as curves over $\mathbb{Q}$, to the projective curve defined by*

$$U^2 + (-2b)V^2 + (b^2 - 4c)W^2 = Z^2, \qquad UW = V^2.$$

Proof. Suppose (x, y, s) is a non-trivial $\overline{\mathbb{Q}}$-solution to $Y^2 S = X(X^2 + bXS + cS^2)$. Let $u = x^2 + bxs + cs^2$. So $xu = y^2 s$ and

$$\begin{aligned}
u^2 &= x^4 + 2bx^3 s + (2c + b^2)x^2 s^2 + 2bcxs^3 + c^2 s^4 \\
u^2 - 2bxsu &= x^4 + (2c - b^2)x^2 s^2 + c^2 s^4 \\
u^2 - 2by^2 s^2 &= x^4 + (2c - b^2)(xs)^2 + c^2 s^4 \\
u^2 - 2b(ys)^2 - (2c - b^2)(xs)^2 &= x^4 + c^2 s^4 \\
u^2 + (-2b)(ys)^2 + (b^2 - 4c)(xs)^2 &= (x^2 - cs^2)^2
\end{aligned}$$

This suggests $(x, y, s) \mapsto (u, v, w, z)$ where

$$u = x^2 + bxs + cs^2, \quad v = ys, \quad w = xs, \quad \text{and} \quad z = x^2 - cs^2.$$

This map extends to a neighborhood of $(0, 1, 0)$: multiply these formulas by x/s giving $u = y^2, v = xy, w = x^2$, and $z = y^2 - cx^2 - 2cxs$.

We need to show an inverse exists. If a point is in the image, under the first formula, we get $u - z - bw = 2cs^2$. So if $u - z - bw \neq 0$, we get $x/s = 2cw/(u - z - bw)$ and $y/s = 2cv/(u - z - bw)$. Thus suggests an inverse map $(u, v, w, z) \mapsto (x, y, s)$ where

$$x = 2cw, \quad y = 2cv, \quad s = u - z - bw.$$

[23] An *isogeny* $E' \to E$ is an algebraically defined homorphism $E'(\overline{\mathbb{Q}}) \to E(\overline{\mathbb{Q}})$ with finite kernel. The size of the kernel is the *degree*.

This does not work at $(1,0,0,1)$. So we multiply the first formula by $u(u+z)/v$ giving us

$$x = 2cv(u+z), \quad y = 2cu(u+z), \quad s = buv + (4c-b^2)vw - bvz.$$

for points in a neighborhood of $(1,0,0,1)$.

We leave it to the reader to check that these function are well-defined algebraic maps between these curves, and that they are indeed inverses. □

Corollary 2. *If $a = d = 1$, then the curve defined by (14) is isomorphic, as projective curves over $\mathbb{Q}$, to the elliptic curve defined by $y^2 = x\big(x^2 - 2bx + (b^2-4c)\big)$.*

Recall, Q_γ is the projective curve defined by (16). By the above corollary, Q_1 is isomorphic to the elliptic curve E' given by $y^2 = x\big(x^2 - 2bx + (b^2-4c)\big)$. So the algebraic map $Q_1 \to E$ considered above yields a map $\varphi' : E' \to E$. Using the explicit descriptions of $Q_\gamma \to E$ and the isomorphism of the above lemma, we can determine the pre-image of the identity under φ': it consists of the identity of E' and the two-torsion point $(0,0)$ of E'. We also see that the other 2-torsion points of E' map to $(0,0)$. A well-known result in the theory of elliptic curves (or more generally, abelian varieties) tells us that, since the identity maps to the identity, φ' is a homomorphism. The kernel has two points, so φ' is a degree 2 isogeny.

As mentioned above, the image of $Q_1(\mathbb{Q})$ is the kernel of $E(\mathbb{Q}) \to \mathbb{Q}^\times / (\mathbb{Q}^\times)^2$. So we get an exact sequence

$$1 \to H' \to E'(\mathbb{Q}) \to E(\mathbb{Q}) \to \mathbb{Q}^\times / \big(\mathbb{Q}^\times\big)^2 \tag{17}$$

where H' is the 2 element subgroup of $E'(\mathbb{Q})$ generated by $(0,0)$.

An interesting thing happends when we carry out this construction with E replaced by E': we get an an isogeny $E'' \to E$, but E'' is clearly isomorphic to E. Thus we get an isogeny $\varphi : E \to E'$ (over $\mathbb{Q}$) of degree 2 and an exact sequence

$$1 \to H \to E(\mathbb{Q}) \to E'(\mathbb{Q}) \to \mathbb{Q}^\times / \big(\mathbb{Q}^\times\big)^2 \tag{18}$$

where H is the 2 element subgroup of $E(\mathbb{Q})$ generated by $(0,0)$.

Lemma 9. *The composition $\varphi' \circ \varphi : E \to E$ is multiplication by ± 2.*

Proof. One could just check this directly using the explicit formulas. But one can avoid this pain by using some basic results from the theory of elliptic curves. First, the $\overline{\mathbb{Q}}$-kernel of an isogeny $E_1 \to E_2$ determines the isogeny uniquely up to a $\mathbb{Q}$-automorphism of E_2 ([15], III, Cor. 4.11). The $\mathbb{Q}$-automorphisms of $\mathbb{Q}$-elliptic curves are just multiplication by ± 1 ([15], III, Cor 10.2). So two isogenies $E \to E$ defined over $\mathbb{Q}$ differ by multiplication by ± 1 if they have the same kernel (over $\overline{\mathbb{Q}}$).

The kernel of $\varphi' \circ \varphi$ is seen to consist of the 2-torsion subgroup. By definition, this is the kernel of the multiplication by 2 isogeny. □

Determining the Rank of $E(\mathbb{Q})$. An application of the above isogenies is finding the rank of (15). We first consider $E(\mathbb{Q})/2E(\mathbb{Q})$ which, by the above lemma, is related to the isogenies φ and φ'. The image of $E(\mathbb{Q}) \to \mathbb{Q}^\times / (\mathbb{Q}^\times)^2$ is finite with every element of order 2. So it has order 2^r for some r. Recall that 2^r is also the number of systems (16) that admit a non-trivial $\mathbb{Q}$-solution.[24] Let $p_1, \ldots, p_r$ be points of $E(\mathbb{Q})$ whose images in $(\mathbb{Q}^\times)^2$ generate the image of $E(\mathbb{Q}) \to \mathbb{Q}^\times / (\mathbb{Q}^\times)^2$.

[24] In practice, one doesn't need to determine the solvability of (16) for every value of γ, but for just enough values to pin down 2^r.

Now repeat this for $E'(\mathbb{Q})$: let the image of $E'(\mathbb{Q}) \to \mathbb{Q}^\times / \left(\mathbb{Q}^\times\right)^2$ have size $2^{r'}$, and let $q_1, \ldots, q_{r'} \in E'(\mathbb{Q})$ correspond to generators of this image.

Use the exact sequences (17) and (18) and the fact that the image of $E(\mathbb{Q})$ under $\varphi' \circ \varphi$ is $2E(\mathbb{Q})$, to conclude that the images of $p_1, \ldots, p_r, \varphi'(q_1), \ldots, \varphi'(q_{r'})$ generate $E(\mathbb{Q})/2E(\mathbb{Q})$. So the order of $E(\mathbb{Q})/2E(\mathbb{Q})$ is at most $2^{r+r'}$. If every 2-torsion point of E is rational, then we claim that this is the exact order: $p_1, \ldots, p_r, \varphi'(q_1), \ldots, \varphi'(q_{r'})$ give linearly independent elements of $V = E(\mathbb{Q})/2E(\mathbb{Q})$ where we consider V as a $\mathbb{F}_2$-vector space. This claim easily reduces to showing that $\varphi'(q_1), \ldots, \varphi'(q_{r'})$ are linearly independent modulo $2E(\mathbb{Q})$. But since every 2-torsion point of E is rational, $(0,0)$ is in the image of $E(\mathbb{Q}) \to E'(\mathbb{Q})$. So any linear dependency of $\varphi'(q_1), \ldots, \varphi'(q_{r'})$ modulo $2E(\mathbb{Q})$ gives one of $q_1, \ldots, q_{r'}$ modulo the image of $E(\mathbb{Q}) \to E'(\mathbb{Q})$. But no such non-trivial dependency exists by the choice of $q_1, \ldots, q_{r'}$ and by the exact sequence (18).

On the other hand, if not every 2-torsion point of E is rational, in other words if $b^2 - 4c$ is not a square, then we can choose $q_{r'} = (0,0)$. Then one can show that $p_1, \ldots, p_r, \varphi'(q_1), \ldots, \varphi'(q_{r'-1})$ gives a basis of $V = E(\mathbb{Q})/2E(\mathbb{Q})$. So in this case $E(\mathbb{Q})/2E(\mathbb{Q})$ has order $r + r' - 1$.

Since $E(\mathbb{Q})$ is a finitely generated abelian group, we can determine its rank from the dimension of $V = E(\mathbb{Q})/2E(\mathbb{Q})$ together with knowledge of the two-torision of $E(\mathbb{Q})$. If 2^k is the size of the two-torsion group of $E(\mathbb{Q})$, then the two-torsion generates a k-dimensional subspace of V. We have two cases: $k = 1$ and $k = 2$. The above calculations imply that in either case, $\dim V - k = r + r' - 2$.

Proposition 9. *The rank of $E(\mathbb{Q})$ is $r + r' - 2$ where r and r' are as above.*

Thus we see that *the $\mathbb{Q}$-solvability of systems of the form (14) are intimately related to the rank of elliptic curves (15).*

Principle Homogeneous Spaces. There is another close relation between the projective curves defined by (14) and elliptic curves. We will see that a curve X defined by (14) is a *principle homogeneous space* for an elliptic curve G in the following sense: the group $G\big(\overline{\mathbb{Q}}\big)$ acts on $X\big(\overline{\mathbb{Q}}\big)$ with one orbit and no non-identity element of $G\big(\overline{\mathbb{Q}}\big)$ has a fixed point. Furthermore, the action is defined algebraically over the field $\mathbb{Q}$.

Before justifying these claims, first observe that

$$(u, v, w, z) \mapsto (a^{1/2} d^{1/2} u, v, a^{-1/2} d^{-1/2} w, dz)$$

is an isomorphism $\psi : X \to X'$ where X is the projective curve defined by (14) and X' is the curve defined by

$$U^2 + bdV^2 + acd^2 W^2 = Z^2, \qquad UW = V^2.$$

Of course, in general ψ is not defined over $\mathbb{Q}$ but over a quadratic extension of $\mathbb{Q}$. By Corollary 2 there is a $\mathbb{Q}$-isomorphism $\chi : X' \to G$ where G is the elliptic curve

$$G: \quad y^2 = x\big(x^2 - 2bdx + (b^2 - 4ac)d^2\big) \tag{19}$$

Proposition 10. *The curve X defined by (14) is a principle homogeneous space for the elliptic curve G defined by (19).*

Proof. Let $\omega = \chi \circ \psi$. So $\omega : X \to G$ is a $\overline{\mathbb{Q}}$-isomorphism between $\mathbb{Q}$-curves. If $g \in G\big(\overline{\mathbb{Q}}\big)$ and $p \in X\big(\overline{\mathbb{Q}}\big)$, define gp as $\omega^{-1}\big(g + \omega(p)\big)$ where $+$ is addition on G. Clearly this gives an action of the group $G\big(\overline{\mathbb{Q}}\big)$ on $X\big(\overline{\mathbb{Q}}\big)$, it is algebraic, it has one orbit, and no non-identity element of $G(\overline{\mathbb{Q}})$ fixes a point of $X(\overline{\mathbb{Q}})$. To show that X is a principle homogeneous space for G, we just need to show that the action is defined over $\mathbb{Q}$.

Suppose $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ sends $\sqrt{ad}$ to $-\sqrt{ad}$. A relatively straightforward calculation using formulas developed above shows that $\omega \circ \sigma \circ \omega^{-1}(g) = \sigma g + (0,0)$ for all $g \in G(\overline{\mathbb{Q}})$. Thus, $\omega(\sigma p) = \omega \circ \sigma \circ \omega^{-1}\big(\omega(p)\big) = \sigma\omega(p) + (0,0)$ for all $p \in X(\overline{\mathbb{Q}})$. So for all $g \in G(\overline{\mathbb{Q}})$ and $p \in X(\overline{\mathbb{Q}})$

$$\omega\sigma\omega^{-1}\big(g + \omega(p)\big) = \sigma\big(g + \omega(p)\big) + (0,0) = \sigma g + \sigma\omega(p) + (0,0) = \sigma g + \omega(\sigma p).$$

This implies that $\sigma(gp) = (\sigma g)(\sigma p)$.

In the other case, where $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ fixes $\sqrt{ad}$, then it is easy even easier to show $\sigma(gp) = (\sigma g)(\sigma p)$. Thus the group action is $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$-invariant. By a standard argument, the action must be defined over $\mathbb{Q}$. □

Since X is a principle homogeneous space for G, the the map $g \mapsto gp$ gives a $\overline{\mathbb{Q}}$-isomorphism between the curves X and G. If X has a rational point p, then this yields a $\mathbb{Q}$-isomorphism between the curve X and G.

If G is an elliptic curve over $\mathbb{Q}$, then the set of $\mathbb{Q}$-isomorphism classes of principle homogeneous spaces for G is denoted WC_G. The set WC_G can be given the structure of a group, and is called the Weil-Châtelet group. The identity element is represented by any principle homogeneous spaces with a rational point. The above proposition implies that X determines an element of WC_G. This element turns out to have order 1 or 2 in WC_G.[25]

The Tate-Shafarevich group $Ш_G$ is the subgroup of WC_G represented by principle homogeneous spaces with $\mathbb{R}$-points and p-adic points for all primes p. Thus *a counter-example to the Hasse Principle of the form (14) considered in this paper gives a concrete representation of an elements of order* 2 *in* $Ш_G$ where G is the elliptic curve given by (19).

Example 4. Lind and Reichardt's counterexample, which we put in the form

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

is a principle homogeneous space for $y^2 = x^3 - 2^4 \cdot 17x$. But this elliptic curve is isomorphic to the elliptic curve E defined by $y^2 = x^3 - 17x$. Thus Lind and Reichardt's counterexample gives an element of order 2 in $Ш_E$.

References

[1] Z.I. Borevich, I.R. Shafarevich, *Number Theory*, Academic Press 1966

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

[3] C. Chevalley, *Démonstration d'une hypothèse de M. Artin*, Abhandl. Sem. Hamburg **11** (1935), 73–75

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

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

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

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

[25] The group structure can be defined cohomologically: one can identify WC_G with the group $H^1\Big(\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}),\, G(\overline{\mathbb{Q}})\Big)$. The formula $\omega \circ \sigma \circ \omega^{-1}(g) = \sigma g + (0,0)$ in the above proof implies that the associated cohomology class has order 1 or 2 since $(0,0)$ has order 2 in $G(\overline{\mathbb{Q}})$.

[8] F. Lemmermeyer, Ö. Öztürün, *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. Silverman, *The Arithmetic of Elliptic Curves*, Springer-Verlag 1986

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

[17] E. Warning, *Bemerkung zur vorstehenden Arbeit von Herrn Chevalley*, Abhandl. Sem. Hamburg **11** (1935), 76–83

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