

# 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. We assume that  $a, b$ , and  $c$  are non-zero integers, and, using a simple argument, we reduce to the case where  $a, b$ , and  $c$  are square-free and pairwise relatively prime. Euler found necessary conditions 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  $|c|$ ,  $-bc$  is a square modulo  $|a|$ , and  $-ca$  is a square modulo  $|b|$ . Lagrange studied the special case  $a = 1$ ; Legendre finally proved that (1) has solutions if and only if Euler's conditions are satisfied, and the young Gauss in his *Disquisitiones Arithmeticae* (Article 294) gave a second proof based on his theory of ternary quadratic forms. There was a large interest in generalizing this result to quadratic forms in arbitrary many variables. Hasse's solution in the 1920s, building on earlier work of Minkowski, was formulated in a very elegant way using the  $p$ -adic numbers developed a few decades earlier by Hensel.

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

$$F_1(X_1, \dots, X_m) = 0 \tag{2}$$

where  $F(X_1, \dots, X_m) \in \mathbb{Z}[X_1, \dots, X_m]$  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 *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). An  $m$ -tuple  $(a_1, \dots, a_m) \in \mathbb{Z}^m$  is said to be *primitive* if for each prime  $p$  there is an  $a_i$  not divisible by  $p$ . 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  $N$ . So a primitive solution modulo  $N$  is a primitive  $m$ -tuple that solves the congruence  $F(X_1, \dots, X_m) \equiv 0 \pmod{N}$ .

An easy way to show that (2) has no non-trivial solution is to show that it has no non-trivial solution in  $\mathbb{R}$ . 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  $F \in \mathbb{Z}[X_1, \dots, X_m]$  is a homogeneous polynomial of degree 2, then  $F(X_1, \dots, X_m) = 0$  has a non-trivial solution in  $\mathbb{Z}^m$  (or, equivalently, in  $\mathbb{Q}^m$ ) if and only if (i) it has a non-trivial solution in  $\mathbb{R}^m$ , and (ii) it has a primitive solution modulo  $N$  for all  $N > 1$ .*

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 non-trivial solution in  $\mathbb{Z}^m$  if and only if (i) it has a non-trivial solution in  $\mathbb{R}^m$ , and (ii) it has a primitive solution modulo  $p^k$  for all primes  $p$  and exponents  $k > 1$ .*

In many cases, finding a solution modulo  $p^k$  reduces, by Hensel’s Lemma (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 a complete metric space, and much of analysis, usually done with  $\mathbb{R}$ , generalizes to  $\mathbb{Q}_p$ . In fact, number theorists often formally introduce a “prime”  $\infty$ , and describe  $\mathbb{R}$  as  $\mathbb{Q}_\infty$ ; the fields  $\mathbb{Q}_p$  for  $p$  a prime or  $\infty$  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  $F \in \mathbb{Z}[X_1, \dots, X_m]$  is homogeneous of degree 2, then  $F(X_1, \dots, X_m) = 0$  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 the equation (2) satisfies the *Hasse Principle* if it has a non-trivial solution in  $\mathbb{Z}^m$  if and only if (i) it has a solution in  $\mathbb{R}^m$ , and (ii) it has a primitive solution modulo  $N$  for each  $N > 0$ . 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.<sup>1</sup>

---

<sup>1</sup>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 polynomials 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 a projective variety defined over  $\mathbb{Q}$  given the existence of  $\mathbb{Q}_p$ -points for all  $p$  (including  $\infty$ ).

A very special case of the Local-Global Principle concerns the equation  $X^2 - aY^2 = 0$  for some nonzero rational number  $a$ . In this example, version 3 of the Hasse Principle states that  $a$  is the square of a rational number if and only if  $a$  is a square in every  $\mathbb{Q}_p$ .

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 [9]:

$$3X^3 + 4Y^3 + 5Z^3 = 0. \quad (3)$$

This cubic obviously has non-trivial solutions in  $\mathbb{R}^3$ , 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*.<sup>2</sup>

Selmer's example not the earliest, nor the simplest: Lind [6] and Reichardt [8] found that the quartic

$$X^4 - 17Y^4 = 2Z^2 \quad (4)$$

gives a counterexample to the Hasse Principle. (The homogeneous version of this type of equation will be discussed in the next section). In contrast to Selmer's example, there are proofs, like the one given in Section 7, that (4) has no non-trivial solutions in  $\mathbb{Z}^3$  involving only quadratic reciprocity — and there are proofs (see e.g. [5]) that require even less. The harder part is to give an elementary proof that (4) has solutions modulo all primes.<sup>3</sup>

The purpose of this expository article is to give a self-contained, accessible proof of the existence of counterexamples, similar to those of Lind and Reichardt's, to the Hasse Principle by using the easy and well-known technique of parametrizing conics. In fact, the only required background is an introductory, undergraduate course in number theory up to quadratic reciprocity, and an introductory, undergraduate course in modern algebra up to basic facts about polynomials over rings and fields. As far as we know, this paper is unique in developing interesting counterexamples to the Hasse Principle in such an elementary manner.<sup>4</sup>

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 (see Mazur [7] for example). As discussed in Appendix B (written for a more advanced audience), these counterexamples are of interest from the point of view of elliptic curves. Our hope is that this paper will give a general mathematical audience a taste of this interesting subject.

---

<sup>2</sup>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 of the elliptic curve  $X^3 + Y^3 + 60Z^3 = 0$  (see also Mazur [7]).

<sup>3</sup>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 not 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.

<sup>4</sup>A less interesting, but simpler counterexample is  $(X^2 - 2Y^2)(X^2 - 17Y^2)(X^2 - 34Y^2) = 0$ . To show that it is a counterexample, use quadratic reciprocity and Propositions 2 and 4.

## 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

$$F_1(X, Y, Z, W) = 0, \quad F_2(X, Y, Z, W) = 0 \quad (5)$$

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 developing interesting counter-examples including those of Lind and Reichardt.<sup>5</sup>

The diophantine systems considered in this paper are of the form

$$aU^2 + bV^2 + cW^2 = dZ^2, \quad UW = V^2 \quad (6)$$

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

$$aX^4 + bX^2Y^2 + cY^4 = dZ^2. \quad (7)$$

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

**Lemma 1.** *The system (6) has a non-trivial solution in  $\mathbb{Z}^4$  if and only if the equation (7) has a non-trivial solution in  $\mathbb{Z}^3$ . Likewise, (6) has a non-trivial solution in  $\mathbb{R}^4$  if and only if (7) has a non-trivial solution in  $\mathbb{R}^3$ .*

*Proof.* If  $(x_0, y_0, z_0)$  is a non-trivial solution to (7) in  $\mathbb{Z}^3$  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 both  $(v_0, w_0, z_0w_0)$  and  $(u_0, v_0, z_0u_0)$  are solution to (7) in  $\mathbb{Z}^3$ . At least one of these must be non-trivial.

This holds when  $\mathbb{Z}$  is replaced by any ring containing  $\mathbb{Z}$ , so it holds for  $\mathbb{R}$ .  $\square$

**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  $(v_0, w_0, z_0w_0)$  and  $(u_0, v_0, z_0u_0)$  are both solution to (7) modulo  $p^k$ . Claim: at least one of  $u_0, v_0$  or  $w_0$  must be prime to  $p^k$ . Otherwise, by assumption  $z_0$  is prime to  $p^k$ , and since  $dz_0^2 \equiv au_0^2 + bv_0^2 + cw_0^2 \pmod{p^k}$ , it follows that  $p^2 \mid d$  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  $(1, v_0u_0^{-1}, z_0u_0^{-1})$  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  $p^k$ .  $\square$

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

<sup>5</sup>An important principle of arithmetic geometry: when classifying a system of diophantine equations do not look at degree alone, but also look at 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  $P_t = \left(\frac{1-t^2}{1+t^2}, \frac{2t}{1+t^2}\right)$ .

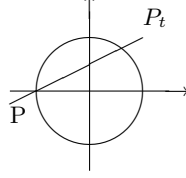


FIGURE 1. Parametrizing the Unit Circle

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

$$(1 - T^2)^2 + (2T)^2 = (1 + T^2)^2. \quad (8)$$

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).<sup>6</sup>

**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  $F[T]$*

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

*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  $\text{char } F \neq 2$ , each of  $q_1, q_2, q_3$  is non-zero, and no two are associates.<sup>7</sup>*

*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  $\text{char } F \neq 2$ . 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.  $\square$

<sup>6</sup>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  $\text{char } F \neq 2$  then every non-degenerate conic can be brought into the form  $ax^2 + by^2 = 1$  with a projective transformation.

<sup>7</sup>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 (coming up with one is another story: see Cremona & Rusin [3]).

**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  $p > 0$ , 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.<sup>8</sup>  $\square$

The proof we have given here goes back to Lagrange, who – in his proof that every positive integer is the sum of four squares – had to prove the solvability of the congruence  $x^2 + y^2 + 1 \equiv 0 \pmod{p}$ .

Figure 2 displays the affine plane over  $\mathbb{F}_7$  (it 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?

We leave it as an exercise to the reader to determine the interior of the unit circle: these are all 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  $(1, 0)$ .

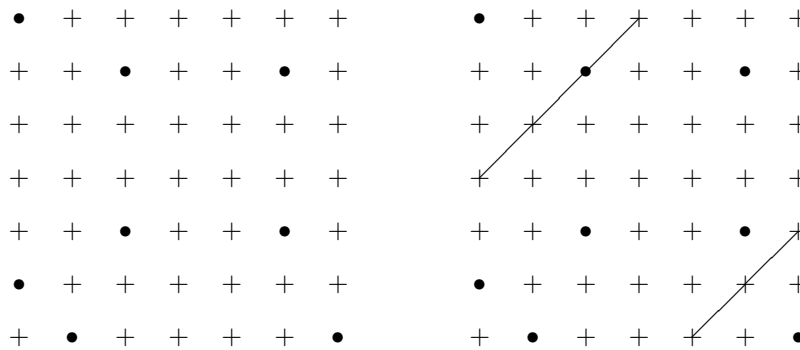


FIGURE 2. The Unit Circle over  $\mathbb{F}_7$ , and its tangent at  $(2, 5)$

<sup>8</sup>This argument 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).

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.<sup>9</sup>

**Proposition 1.** *Let  $f, g \in \mathbb{F}_p[X]$  be non-zero polynomials of degree at most two. If  $(\frac{f(t)}{p}) = (\frac{g(t)}{p})$  for all  $t \in \mathbb{F}_p$  then  $f$  and  $g$  are associates.*

*Proof.* By Euler's criterion,  $(\frac{f(t)}{p}) = f(t)^{(p-1)/2}$  and  $(\frac{g(t)}{p}) = g(t)^{(p-1)/2}$ . So, if  $(\frac{f(t)}{p}) = (\frac{g(t)}{p})$  for all  $t \in \mathbb{F}_p$ , then every  $t \in \mathbb{F}_p$  is a root of  $f^{(p-1)/2} - g^{(p-1)/2}$ . 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.  $\square$

**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  $(\frac{q_1(t)}{p}) \neq -(\frac{q_2(t)}{p})$ . So  $(\frac{q_1(t)q_2(t)}{p}) \neq -1$ ; in other words,  $q_1(t)q_2(t) = c^2$  for some  $c \in \mathbb{F}_p$ . In addition,  $q_1(t)$  and  $q_2(t)$  are not both 0.

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

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  $r$ th power modulo  $p$ , then  $N$  is an  $r$ th power modulo  $p^k$  for all  $k \geq 1$ .*

*Proof.* (By induction on  $k$ ). Suppose that  $N \equiv a^r \pmod{p^k}$ . Write  $N - a^r = cp^k$ . Using the binomial expansion,  $(a + xp^k)^r \equiv a^r + ra^{r-1}xp^k \pmod{p^{k+1}}$ .

So  $N - (a + xp^k)^r \equiv (c - ra^{r-1}x)p^k \pmod{p^{k+1}}$ . Observe  $(p, a) = 1$  since  $(p, N) = 1$ . So there is an  $x$  such that  $p \mid (c - ra^{r-1}x)$ , and  $N \equiv (a + xp^k)^r \pmod{p^{k+1}}$ .  $\square$

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,  $d^{-1}aX^4 + d^{-1}cY^4 = Z^2$  has a non-trivial solution  $(x_1, y_1, z_1)$  modulo  $p$ .

If  $z_1 \not\equiv 0 \pmod{p}$  then let  $N = d^{-1}(ax_1^4 + cy_1^4)$ . By Proposition 2,  $N \equiv n^2 \pmod{p^k}$  for some  $n \in \mathbb{Z}$ , and  $(x_1, y_1, n)$  is a solution modulo  $p^k$ . If  $x_1 \not\equiv 0 \pmod{p}$ , then let  $x_1^{-1}$  be an inverse to  $x_1$  modulo  $p^k$ . Then  $(1, y_1x_1^{-1}, nx_1^{-2})$  is a primitive solution modulo  $p^k$ . If  $x_1 \equiv 0 \pmod{p}$ , then take  $(x_1y_1^{-1}, 1, ny_1^{-2})$  instead.

<sup>9</sup>Everything in this section extends easily to finite fields of odd order, not just prime fields.

If  $z_1 \equiv 0 \pmod{p}$ , let  $c^{-1}$  be an inverse for  $c$  modulo  $p^k$ . The existence of a non-trivial solution with  $z_1 \equiv 0 \pmod{p}$  implies that  $N = -ac^{-1}$  is a non-zero fourth power modulo  $p$ . By Proposition 2, there is an  $n$  such that  $N \equiv n^4 \pmod{p^k}$ , and  $(1, n, 0)$  is a primitive solution modulo  $p^k$ .  $\square$

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

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

*Proof.* (By induction). Suppose  $N \equiv a^4 \pmod{2^k}$  where  $k \geq 4$ . Write  $N - a^4 = c2^k$ . Using the binomial expansion gives  $(a + x2^{k-2})^4 \equiv a^4 + a^3x2^k \pmod{2^{k+1}}$ .

So  $N - (a + x2^{k-2})^4 \equiv (c - a^3x)2^k \pmod{2^{k+1}}$ . Observe  $(2, a) = 1$  since  $(2, N) = 1$ . So there is an  $x$  such that  $2 \mid (c - a^3x)$ , and  $N \equiv (a + x2^{k-2})^4 \pmod{2^{k+1}}$ .  $\square$

## 6. SOLUTIONS MODULO $p^k$

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

$$U^2 - qW^2 = dZ^2, \quad UW = V^2 \quad (10)$$

where

- (1)  $q$  is a prime such that  $q \equiv 1 \pmod{16}$ ,
- (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 Lemma 2, to find primitive solutions modulo  $p^k$ , it suffices to find primitive solutions modulo  $p^k$  to the equation  $X^4 - qY^4 = dZ^2$ . If  $p$  does not divide  $2dq$ , then  $X^4 - qY^4 = dZ^2$  has a primitive solution modulo  $p^k$  by Proposition 3.

Suppose  $p = q$ . Since  $d$  is a non-zero square modulo  $q$ , Proposition 2 implies that  $d \equiv n^2 \pmod{q^k}$  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  $p \mid c$  where  $p$  is odd. Then, by Proposition 2,  $q \equiv n^4 \pmod{p^k}$  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  $q \equiv n^4 \pmod{2^k}$ , and  $(n, 1, 0)$  is a solution to  $X^4 - qY^4 = dZ^2$  modulo  $2^k$ .  $\square$

## 7. COUNTEREXAMPLES TO THE HASSE PRINCIPLE

Consider the diophantine equation  $X^4 - qY^4 = dZ^2$  where  $q \equiv 1 \pmod{8}$  is a prime and where  $d$  is square-free and prime to  $q$ . We begin by developing a necessary condition for this equation to have a non-trivial solution in  $\mathbb{Z}^3$ . 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 solution  $(x_0, y_0, z_0)$  in  $\mathbb{Z}^3$  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  $x_1^4 - qy_1^4 \equiv 0 \pmod{p}$ , implies that  $\left(\frac{q}{p}\right) = 1$ . By quadratic reciprocity,  $\left(\frac{p}{q}\right) = 1$  for all such  $p$ . Now  $q \equiv 1 \pmod{8}$ , so  $-1$  and  $2$  are quadratic residues modulo  $q$ . Thus  $z_1$  is the product of quadratic residues:  $\left(\frac{z_1}{q}\right) = 1$ . The congruence  $d \equiv z_1^{-2}x_1^4 \pmod{q}$  now implies that  $d$  is a fourth power modulo  $q$ . To summarize:

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

$$U^2 - qW^2 = dZ^2, \quad UW = V^2 \quad (11)$$

where

- (1)  $q$  is a prime such that  $q \equiv 1 \pmod{16}$ ,
- (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 2, and Lemma 1 together gives us our main result.

**Theorem 3.** *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 3:

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

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<sup>10</sup>  $q \equiv 1 \pmod{16}$  and such that  $2$  is not a fourth power modulo  $q$ . Of course,  $\left(\frac{2}{q}\right) = 1$ , so

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

gives a counterexample to the Hasse Principle.<sup>11</sup>

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

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

<sup>10</sup>Actually the result holds for all primes  $q \equiv 1 \pmod{8}$ , as can easily be seen by looking at the 2-adic case in the proof of Prop. 5: if  $d = 2$ , then there is a solution with  $Y = 1$  and  $Z = 2$ .

<sup>11</sup>This actually gives an infinite number of examples. The density,  $1/16$ , of such primes  $q$  can be obtained using the Chebotarev Density Theorem with  $\text{Gal}(\mathbb{Q}(\zeta_{16}, 2^{1/4})/\mathbb{Q})$ .

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  $p$  (or, more exactly, small powers of  $p$ ) to solutions modulo  $p^k$  for all  $k$ . Hensel's Lemma is closely connected to Newton's method from calculus. Here is a basic version.

**I deleted the footnote**

The idea of introducing the  $p$ -adic numbers as a completion with respect to some metric is due to Kürschak and Ostrowski. Hensel introduced  $p$ -adic numbers only formally.

**Proposition 6** (Hensel's Lemma). *Let  $f \in \mathbb{Z}[T]$  be a polynomial with derivative  $f'$ . If  $t_1 \in \mathbb{Z}$  is such that  $f(t_1) \equiv 0 \pmod{p}$  but  $f'(t_1) \not\equiv 0 \pmod{p}$ , then for all  $k \geq 1$  there is a  $t_k \in \mathbb{Z}$  such that  $t_k \equiv t_1 \pmod{p}$  and  $f(t_k) \equiv 0 \pmod{p^k}$ .*

*Proof.* (By Induction) Assume that  $t_k \equiv t_1 \pmod{p}$  and  $f(t_k) \equiv 0 \pmod{p^k}$ . Then we have  $f(t_k) = ap^k$  for some integer  $a$ , and if  $p \mid a$  we are done: let  $t_{k+1} = t_k$ . If  $p \nmid a$ , we can try to modify  $t_k$  modulo  $p^k$ , that is, we put  $t_{k+1} = t_k + xp^k$ ; our goal is to determine  $x$  in such a way that we get  $f(t_{k+1}) \equiv 0 \pmod{p^{k+1}}$ .

By the following Lemma and Corollary,

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

We can choose  $x$  to make the right hand side vanish since  $p \nmid f'(t_k)$ . □

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  $f(dp^k + c) \equiv f(c) + f'(c)dp^k \pmod{p^{k+1}}$  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  $(a_1, a_2, a_3, \dots)$  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  $\mathbb{Z}/p^{k+1}\mathbb{Z} \rightarrow \mathbb{Z}/p^k\mathbb{Z}$  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 is denoted by  $\mathbb{Q}_p$ . There is a natural injective ring homomorphism  $\mathbb{Z} \rightarrow \mathbb{Z}_p$  defined by sending  $a$  to  $(a_1, a_2, \dots)$  where  $a_k$  is the natural 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  $(a_1, a_2, \dots)$  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 metric space with some rather interesting properties. For an introduction to the  $p$ -adic numbers, with prerequisites similar to those of the current paper, see [4].

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. 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  $x^2 + y^2 \equiv 1 \pmod{27}$  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

$$(1, 0) \text{ --- } (1, 3) \text{ --- } (10, 12) \text{ --- } \dots,$$

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

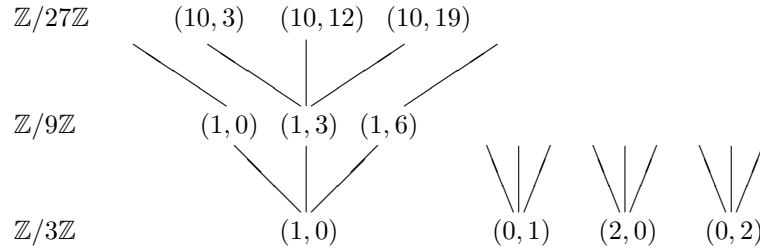


FIGURE 3. The Unit Circle over  $\mathbb{Z}_3$

A  $p$ -adic solution to a polynomial equation  $f(X_1, \dots, X_m) = 0$ , where  $f$  has integer coefficients, gives simultaneously a solution to  $f(X_1, \dots, X_m) \equiv 0 \pmod{p^k}$  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 the results of this paper, for example Proposition 5 or Hensel’s Lemma (Proposition 6), we ignored coherence among solutions modulo  $p^k$ . If we had been more careful, we could have demonstrated the existence of a coherent sequence of solutions. The following shows that that is not necessary: we can always be assured of 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

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

Let  $(x_1, y_1, z_1), (x_2, y_2, z_2), (x_3, y_3, z_3), \dots$  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  $x = (a_1, a_2, \dots)$  where  $a_k$  is the image of  $x'_k$  in  $\mathbb{Z}/p^k\mathbb{Z}$ . Define  $y$  and  $z$  in a similar manner.  $\square$

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*. Similarly, Hensel's Lemma can be stated as follows:

**Proposition 7** (Hensel's Lemma: version 2). *Let  $f \in \mathbb{Z}[T]$  be a polynomial with derivative  $f'$ . If  $t \in \mathbb{Z}$  is such that  $f(t) \equiv 0 \pmod{p}$  but  $f'(t) \not\equiv 0 \pmod{p}$ , then there is a  $u \in \mathbb{Z}_p$  such that  $f(u) = 0$  and such that  $u$  and  $t$  agree modulo  $p$ .*

*Remark.* The proof generalizes easily for  $f \in \mathbb{Z}_p[T]$ . Stronger forms of Hensel's Lemma address the case where  $f'(t) \equiv 0 \pmod{p}$ .

## APPENDIX B: 2-DESCENT ON ELLIPTIC CURVES

The systems of equations considered in this paper do not function merely as assessable counterexamples to the Hasse Principle, but arise very naturally in the computation of Mordell-Weil ranks of elliptic curves. In this appendix, we assume some familiarity with elliptic curves on the part of the reader.

Assume that we have an elliptic curve in Weierstrass form with a point of order 2:

$$E : y^2 = x(x^2 + ax + b).$$

When using the technique of 2-descent to approximate the Mordell-Weil ranks of  $E$ , one needs to decide whether or not

$$b_1U^2 + aV^2 + b_2W^2 = Z^2, \quad UW = V^2 \tag{12}$$

has a non-trivial  $\mathbb{Z}$ -solution where where  $b_1, b_2$  run through the factors of  $b = b_1b_2$ . As a first step, one tries to decide if it has primitive solutions modulo prime powers. The main result of this Appendix, a generalization of Proposition 3, is an elementary proof for local solvability outside a certain finite set of primes (those with bad reduction).<sup>12</sup>

Our main result is

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

*Proof.* This follows from Lemma 2 and Proposition 8 below.  $\square$

For the proof of Proposition 8 we need a generalization of Theorem 1:

**Theorem 5.** *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.*

<sup>12</sup>See Silverman [11], Chapter X for a (much more advanced) discussion on the use of descent to compute the rank of elliptic curves.

*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

$$f(q'_1, q_2) = a\left(q_1 - \frac{b}{2a}q_2\right)^2 + b\left(q_1 - \frac{b}{2a}q_2\right)q_2 + cq_2^2 = aq_1^2 + \left(c - \frac{b^2}{4a}\right)q_2^2 = q_3^2.$$

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  $q'_1(t)q_2(t) = d^2$  for some  $d \in \mathbb{F}_p$ , and  $q'_1(t)$  and  $q_2(t)$  are not both 0.

Suppose that  $q'_1(t) \neq 0$ . Then  $(q'_1(t), d, q'_1(t)q_3(t))$  is a non-trivial solution to  $f(X^2, Y^2) = Z^2$ . If  $q_2(t) \neq 0$  then  $(d, q_2(t), q_2(t)q_3(t))$  is a non-trivial solution.  $\square$

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

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

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

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

*Proof.* Let  $f$  be the polynomial  $aX^2 + bXY + cY^2$ . By Theorem 5, the equation  $f(X^2, Y^2) = Z^2$  has a non-trivial solution  $(x_1, y_1, z_1)$  modulo  $p$ .

If  $z_1 \not\equiv 0 \pmod{p}$  then, by Proposition 2,  $f(x_1^2, y_1^2) \equiv n^2 \pmod{p^k}$  for some  $n \in \mathbb{Z}$ , and  $(x_1, y_1, n)$  is a solution modulo  $p^k$ . If  $x_1 \not\equiv 0 \pmod{p}$ , then let  $x_1^{-1}$  be an inverse of  $x_1$  modulo  $p^k$ . Then  $(1, y_1x_1^{-1}, nx_1^{-2})$  is a primitive solution modulo  $p^k$ . If  $x_1 \equiv 0 \pmod{p}$ , then take  $(x_1y_1^{-1}, 1, ny_1^{-2})$  instead.

If  $z_1 \equiv 0 \pmod{p}$ , then  $x_1y_1^{-1}$  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  $f(t^2, 1) \equiv 0 \pmod{p^k}$ . Thus  $(t, 1, 0)$  is the desired solution.  $\square$

## APPENDIX C: CURVES OVER FINITE FIELDS

A major purpose for this paper is to make the concept of local solvability accessible to a wider audience. So naturally, the results we used are just easy special cases of important, but harder to prove, results in the algebraic geometry of curves over a finite field. The following remarks are for the benefit of the reader who wishes to gain a deeper understanding of this interesting subject.

Lemma 4 is a very special case of the Theorem of Chevalley–Warning<sup>13</sup> (see [1, p. 6] or [10, Chap. 1, § 2] for textbook versions, or [2] and [12] for the original publications).

<sup>13</sup>Some sources call it the theorem of Chevalley–Waring, confusing Ewald Warning (1910 – 1999) with the more famous Edward Waring (1736 – 1798).

Theorems 1 and 5 are special cases of a general theorem due to F. K. Schmidt (also proved by Châtelet) according to which any smooth curve of genus 1 has a point over any finite field. Schmidt's proof used zeta functions of function fields and the theorem of Riemann-Roch.

In fact, the system (6) defines a non-singular curve  $C$  of genus 1 in  $\mathbb{P}^3$ , and when  $p \nmid acd(b^2 - 4ac)$ , this curve reduces modulo  $p$  to a non-singular curve of genus 1 defined over  $\mathbb{F}_p$ . One way to see that (6) defines a curve  $C$  of genus 1 is to consider the map  $(u_0, v_0, w_0, z_0) \mapsto (u_0, v_0, w_0)$ . This map can be seen to send  $C$  to the plane conic  $D$  defined by the equation  $UW = V^2$ . The map  $C \rightarrow D$  is two to one, except at four points of ramification. The Riemann-Hurwitz formula, and the fact that  $D$  has genus 0, tells us that the genus of  $C$  is 1.

Once we know that  $C$  has an  $\mathbb{F}_p$ -point due to F. K. Schmidt's Theorem, we can use Lemma 2 (and the remark following the Lemma) to get Theorems 1 and 5.

F. K. Schmidt's Theorem, and hence Theorems 1 and 5, follow from the Hasse-Weil bound for curves of genus 1, according to which the number  $N_q$  of  $\mathbb{F}_q$ -rational points on a smooth projective curve of genus 1 satisfies  $|N_q - (q + 1)| \leq 2\sqrt{q}$ . Observe that  $N_q \leq 1$  implies that  $q \leq 2\sqrt{q}$ , which in turn implies that  $q \leq 4$ ; thus for primes  $q \geq 5$  there is at least one affine point on  $C$ . For  $q = 3$  and the curves considered in Theorems 1 and 5, this can be shown by a direct calculation.

#### REFERENCES

- [1] Z.I. Borevich, I.R. Shafarevich, *Number Theory*, Academic Press 1966
- [2] C. Chevalley, *Démonstration d'une hypothèse de M. Artin*, Abhandl. Sem. Hamburg **11** (1935), 73–75
- [3] J.E. Cremona, D. Rusin, *Efficient solution of rational conics*, Math. Comp. **72** (2003), no. 243, 1417–1441
- [4] F. Q. Gouvêa, *p-adic Numbers*, Springer-Verlag 1997 (second edition)
- [5] F. Lemmermeyer, Ö. Öztürün, *Euler's Trick and Second 2-Descents*, preprint
- [6] C.-E. Lind, *Untersuchungen über die rationalen Punkte der ebenen kubischen Kurven vom Geschlecht Eins*, Diss. Univ. Uppsala 1940
- [7] B. Mazur, *On the passage from local to global in number theory*, Bull. Amer. Math. Soc. (N.S.) **29** (1993), no. 1, 14–50
- [8] H. Reichardt, *Einige im Kleinen überall lösbare, im Großen unlösbare diophantische Gleichungen*, J. Reine Angew. Math. **184** (1942), 12–18
- [9] E. Selmer, *The diophantine equation  $ax^3 + by^3 + cz^3 = 0$* , Acta Math. **85** (1951), 203–362
- [10] J.-P. Serre, *A course in arithmetic*, Springer-Verlag 1973
- [11] J. Silverman, *The arithmetic of elliptic curves*, Springer-Verlag 1986
- [12] E. Warning, *Bemerkung zur vorstehenden Arbeit von Herrn Chevalley*, Abhandl. Sem. Hamburg **11** (1935), 76–83