SIMPLE COUNTEREXAMPLES TO THE LOCAL-GLOBAL PRINCIPLE

W. AITKEN, F. LEMMERMEYER

Abstract. After Hasse had found the first example of a Local-Global principle in the 1920s by showing that a quadratic form in n variables represented 0 in rational numbers if and only if it did so in every completion of the rationals, mathematicians investigated whether this principle held in other situations. Among the first counterexamples to the Hasse principle were curves of genus 1 constructed by Lind and Reichardt: these were curves without rational points but with points in every completion of $\mathbb{Q}$. In this article we will show that the technique of rational parametrization of conics is powerful enough to derive Reichardt's result.

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: Euler found a necessary condition for solvability in nonzero integers (or, which is the same, in nonzero rational numbers): $-ab \equiv r^2 \bmod c$; $-bc \equiv s^2 \bmod a$; and $-ca \equiv t^2 \bmod b$. Lagrange studied the special case $a = 1$; Legendre finally proved that (1) has solutions if and only if Euler's conditions are satisfied, and Gauss 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 realized that the general result could be formulated in a very elegant way.

In fact, Hasse used the language of p-adic numbers invented by Hensel; in this language, an equation such as (1) has a nontrivial solution in $\mathbb{Q}_p$ if and only if the congruence $aX^2 + bY^2 + cZ^2 \equiv 0 \bmod p^k$ has a nontrivial solution for every $k \geq 1$. In addition to the usual primes p we also introduce the symbolic prime $p = \infty$ and put $\mathbb{Q}_\infty = \mathbb{R}$. Hasse then found that the known criteria for the solvability of (1) could be expressed by the following Local-Global Principle:

> (1) is solvable globally (that is, has a nontrivial solution in the field $\mathbb{Q}$ of rational numbers) if and only if it is everywhere locally solvable (that is, in every completion $\mathbb{Q}_p$ of $\mathbb{Q}$).

Hasse also proved that this result even holds for quadratic forms of an arbitrary number of variables.

Geometrically, equation (1) describes a conic in the projective plane, and Hasse's Local-Global Principle guarantees that this conic has a rational point (a point whose coordinates are rational numbers) if and only if it has $\mathbb{Q}_p$-rational points for every p. In this form, the Local-Global Principle does not generalize to curves of higher

degree: Selmer found [5] that the cubic curve

$$3X^3 + 4Y^3 + 5Z^3 = 0 \tag{2}$$

has $\mathbb{Q}_p$-rational points for every p (this is an easy exercise) but does not have a rational point (this is not trivial: known proofs use the arithmetic of the cubic number field $\mathbb{Q}(\sqrt[3]{60})$). This work of Selmer led to the notion of Selmer groups and Tate-Shafarevich groups in the theory of elliptic curves, and Selmer's example can nowadays be interpreted as an element of order 3 in the Tate-Shafarevich group of the elliptic curve $X^3 + Y^3 + 60Z^3 = 0$.

Counterexamples to the Hasse principle simpler than Selmer's had been constructed before by Lind [2] and Reichardt [4]: they found that the quartic

$$2Z^2 = X^4 - 17Y^4 \tag{3}$$

has nontrivial local solutions everywhere but has no nontrivial rational point. In this case it is quite easy to see that there is no rational solution: the standard proof involves quadratic reciprocity, and there are proofs (see e.g. [1]) that require even less. The hard part here is to show that (3) has local solutions everywhere; the simplest approach uses quartic Gauss and Jacobi sums. Applied to general quartics like

$$\mathcal{T} : N^2 = b_1M^4 + aM^2e^2 + b_2e^4, \tag{4}$$

this method only shows the solvability for sufficiently large values of p. In this article we will show that a precise criterium for the local solvability of (4) can be derived using the well known technique of parametrizing conics.

2. Parametrizing Conics

A conic is a curve of degree 2 in the affine plane; we will only have to deal with conics of the form $y^2 = b_1x^2 + ax^2 + b_2$, where the coefficients a, b_1, b_2 lie in some field K (in our case $\mathbb{F}_p$). Such a quadratic equation will in general describe ellipses, parabolas or hyperbolas; conics such as $y^2 = x^2$, however, are just a pair of lines. Note that the lines may be defined over a quadratic extension of K: the conic $y^2 = 2$ is defined over $\mathbb{Q}$, and consists of two lines $y = \sqrt{2}$ and $y = -\sqrt{2}$ defined over $\mathbb{Q}(\sqrt{2})$. Such conics are called degenerate, and we claim

Lemma 1. *The conic $y^2 = f(x)$, where $f(x) = b_1x^2 + ax^2 + b_2 \in K[x]$ and K is a field of characteristic $\neq 2$, is degenerate if and only if $a^2 - 4b_1b_2 = 0$.*

Proof. If the conic is a pair of lines, then $y^2 - f(x) = (y - rx - s)(y - tx - u)$. Comparing coefficients implies that $r + t = s + u = 0$, hence $y^2 - f(x) = (y - rx - s)(y + rs + x)$, and then $a^2 - 4b_1b_2 = 0$.

Conversely, assume that $a^2 - 4b_1b_2 = 0$. If $b_1 = 0$, then $a = 0$ as well, hence the conic has equation $y^2 = b_2$, hence is a pair of lines (defined over $K(\sqrt{b_2})$). If $b_1 \neq 0$, then $4b_1f(x) = (2b_1x + a)^2$, hence the conic can be written in the form $4b_1y^2 = (2b_1x + a)^2$, and again this is a pair of lines, where the equations of the lines have coefficients in $K(\sqrt{b_1})$. □

For nonsingular conics defined over some field K it is easy to determine all points (x, y) on the conic with coordinates in K from one known such point:

Lemma 2. *Consider the conic $C : Y^2 = f(X)$ for $f(X) = b_1X^2+aX+b_2 \in K[X]$. Assume that $y_0^2 = f(x_0)$ for $x_0, y_0 \in K$. Then every point $(x, y) \in K \times K$ with $x \neq x_0$ is given by*

$$x = \frac{t^2x_0 - 2ty_0 + b_1x_0 + a}{t^2 - b_1}, \quad y = \frac{-t^2y_0 + t(2b_1x_0 + a) - b_1y_0}{t^2 - b_1} \tag{5}$$

for some $t \in K \setminus \{\pm\sqrt{b_1}\}$.

Proof. Starting with the K-rational point $P = (x_0, y_0)$ we can parametrize the conic C: consider all lines L_t through P with 'slope' $t \in K$; then $L_t : y = t(x - x_0) + y_0$ intersects the conic in P and in a second point with coordinates (x, y). Plugging the equation of L_t into that of C we find $(t(x - x_0) + y_0)^2 = b_1x^2 + ax + b_2$. Since $x = x_0$ is a root of this quadratic equation in x_0, we can factor out $(x-x_0)$. In fact

$$t^2(x - x_0)^2 + 2ty_0(x - x_0) + b_1x_0^2 + ax_0 + b_2 = b_1x^2 + ax + b_2$$

shows that

$$(x - x_0)(t^2(x - x_0) + 2ty_0 - b_1(x + x_0) - a).$$

The root $x = x_0$ of the first factor corresponds to (x_0, y_0); the second factor vanishes if and only if $(t^2 - b_1)x = t^2x_0 - 2ty_0 + b_1x_0 + a$, and this leads to the formulas (5).

Clearly every value $t \in K$ with $t^2 \neq b_1$ provides a K-rational point on the conic. Conversely, if (x, y) is a point on the conic with coordinates in K and $x \neq x_0$, then it comes from $t = \frac{y-y_0}{x-x_0}$. □

3. Quartics over $\mathbb{F}_p$

Consider the quartic $\mathcal{T}$, with b_1 a squarefree integer, over the field $\mathbb{F}_p$. Our aim is to prove the following

Theorem 1. *The quartic (4) has an $\mathbb{F}_p$-rational point for every prime p such that $p \nmid 2(a^2 - 4b_1b_2)$.*

Remark. This is a special case 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.

Proof of Theorem 1. If equation (4) has a solution (N, M, e) in $\mathbb{F}_p$ with $e = 0$, then $N^2 \equiv b_1M^4 \bmod p$, and this implies that b_1 is a square modulo p (possibly 0). Conversely, if b_1 is a square modulo p, then there exists an $\mathbb{F}_p$-rational point $(N, M, e) \in \mathbb{F}_p \times \mathbb{F}_p \times \mathbb{F}_p$ with $e = 0$ (and $M \neq 0$).

Thus Theorem 1 is proved if b_1 is a square modulo p, so from now on we will assume that $(b_1/p) = -1$. In this case we can't have solutions with $e = 0$, so we might as well divide through by e^4, put $y = N/e^2$ and $X = M/e$, and get

$$y^2 = b_1X^4 + aX^2 + b_2. \tag{6}$$

Now the substitution $X^2 = x$ transforms (6) into the conic

$$C : y^2 = b_1x^2 + ax + b_2. \tag{7}$$

The condition $p \nmid 2(a^2 - 4b_1b_2)$ ensures that C is nonsingular, and that we can find all $\mathbb{F}_p$-rational points on C once we know one. Our aim is to find an $\mathbb{F}_p$-rational point (x, y) on C such that $x = X^2$ is a square.

The proof proceeds in several steps:

(1) *The conic C has an $\mathbb{F}_p$-rational point.* Assume not; then the right hand side of (7) is a nonsquare for every $x \in \mathbb{F}_p$. Thus, by Euler's criterion, $f(X) = (b_1X^2 + aX + b_2)^{(p-1)/2} + 1$ is a polynomial of degree $p-1$ with $f(x) = 0$ for all $x \in \mathbb{F}_p$: this is a contradiction because polynomials f over fields have at most $\deg f$ roots.

(2) *Parametrize the conic C.* Applying Lemma 2 we find that all $\mathbb{F}_p$-rational points on C with $x \neq x_0$ are given by (5). Since we assumed that b_1 is a nonsquare modulo p, every $t \in \mathbb{F}_p$ gives rise to a point on C over $\mathbb{F}_p$. If $x_0 = 0$, then x_0 is a square and we are done. If $x_0 \neq 0$, then we can multiply the numerator and denominator in (5) by x_0 and get

$$x = \frac{(x_0t - y_0)^2 - b_2}{x_0(t^2 - b_1)}. \tag{8}$$

(3) *There is a point (x, y) on C with $x = X^2$.* Assume that there is no point $(x, y) \in \mathbb{F}_p \times \mathbb{F}_p$ on C with $x \in \mathbb{F}_p^2$; then we must have $(x/p) = -1$ for all x, in particular $(x_0/p) = -1$ and therefore $\left(\frac{(x_0t-y_0)^2-b_2}{p}\right) = \left(\frac{t^2-b_1}{p}\right)$ for all $t \in \mathbb{F}_p$.

By Corollary 1 below we have $y_0 = 0$ and $b_2 = x_0^2b_1$. This gives $0 = y_0^2 = b_1x_0^2 + ax_0 + b_2 = b_1x_0^2 + ax_0 + b_1x_0^2$, hence $a = -2b_1x_0$. But then $a^2 - 4b_1b_2 = 0$ contradicting the assumption.

The proof of Theorem 1 is now complete. □

It remains to prove Corollary 1 below. We start with

Lemma 3. *Let $f, g \in \mathbb{F}_p[X]$ be quadratic polynomials over $\mathbb{F}_p$. If $f(t)^n = g(t)^n$ for all $t \in \mathbb{F}_p$ and some integer $n \leq \frac{p-1}{2}$, then there exists a constant $c \in \mathbb{F}_p$ such that $f = c \cdot g$.*

Proof. Clearly $\deg f^n = n \deg f \leq p - 1$, hence the polynomial $f^n - g^n$ has degree $\leq p - 1$ and at least p roots $0, 1, \ldots, p - 1$. Since $\mathbb{F}_p$ is a field, polynomials of degree m have at most m roots; hence we conclude that $f^n = g^n$.

Now factor f and g into linear factors over some finite extension of $\mathbb{F}_p$; then every root α with multiplicity m is a root of multiplicity mn of f^n, thus of g^n, hence a root of multiplicity m of g. Thus f and g have the same roots (with multiplicity) over some extension of $\mathbb{F}_p$, hence they are equal up to some constant c (which necessarily is an element of the base field $\mathbb{F}_p$ since the coefficients of f and g are). □

Proposition 1. *Assume that $f, g \in \mathbb{F}_p[X]$ are quadratic polynomials over $\mathbb{F}_p$ such that $(\frac{f(t)}{p}) = (\frac{g(t)}{p})$ for all $t \in \mathbb{F}_p$. Then there exists a constant $c \in \mathbb{F}_p$ such that $f = c \cdot g$.*

Proof. By Euler's criterion we know that $(\frac{f(t)}{p}) \equiv f(t)^n \pmod p$ with $n = \frac{p-1}{2}$; thus the assumptions imply that $f(t)^n \equiv g(t)^n \pmod p$ for all $t \in \mathbb{F}_p$, so the claim follows from Lemma 3. □

Corollary 1. *If $\left(\frac{(x_0t-y_0)^2-b_2}{p}\right) = \left(\frac{t^2-b_1}{p}\right)$ for $t = 0, 1, \ldots, p-1$, then $y_0 = 0$ and $b_2 = b_1x_0^2$.*

Proof. The converse of the claim is trivially true. On the other hand, applying Prop. 1 to the assumption shows that $f(X) = (x_0X - y_0)^2 - b_2$ and $g(X) = X^2 - b_1$ differ

by a constant factor c; comparing the coefficients of the leading term shows that $c = x_0^2$ whereas comparing linear terms gives $y_0 = 0$. Finally, comparing constant terms shows that $b_2 = b_1 x_0^2$. □

4. The Hensel Lift

In the preceding section we have studied the existence of $\mathbb{F}_p$-rational points on curves $Y^2 = f(X)$ for a quartic polynomial f. Here we will investigate whether these points can be lifted to solutions in the p-adic numbers.

To this end, consider the equation $Y^2 - f(X) = 0$, where $f \in \mathbb{Z}[X]$ is a polynomial with integral coefficients. Assume that we can find integers $x, y \in \mathbb{Z}$ with $y^2 - f(x) \equiv 0 \bmod p$; we would like to lift this to a solution modulo higher powers of p.

This will be done by induction, so let us assume that we are given a solution modulo p^k, that is, integers x_k, y_k with $y_k^2 - f(x_k) \equiv 0 \bmod p^k$. Then we will have $y_k^2 - f(x_k) = ap^k$ for some integer a, and if $p \mid a$ we are done. If $p \nmid a$, we can try to modify x_k and y_k modulo p^k, that is, we put $x_{k+1} = x_k + rp^k$ and $y_{k+1} = y_k + sp^k$; our goal is to determine r and s in such a way that we get $y_{k+1}^2 - f(x_{k+1}) \equiv 0 \bmod p^{k+1}$. Now

$$\begin{aligned} y_{k+1}^2 - f(x_{k+1}) &\equiv y_k^2 + 2sy_kp^k - f(x_k) - rf'(x_k)p^k \\ &\equiv (a + 2sy_k - rf'(x_k))p^k \bmod p^{k+1}. \end{aligned}$$

Thus we can make the right hand side vanish unless $p \mid y_k$ and $p \mid f'(x_k)$. Since $p \mid (y_k - f(x_k))$ by assumption, this means that $x_k \bmod p$ is a root of both f and f' in $\mathbb{F}_p$, which in turn implies that $p \mid \operatorname{disc} f$. We have shown:

Lemma 4 (Hensel's Lemma)**.** *Let $f \in \mathbb{Z}[X]$ be a polynomial; if p is a prime with $p \nmid 2 \operatorname{disc} f$, then every solution of $Y^2 - f(X) \equiv 0 \bmod p$ can be lifted to a solution modulo p^k for any $k \geq 1$.*

The polynomial $f(X) = b_1X^4 + aX^2 + b_2$ has discriminant $\operatorname{disc} f = 16b(a^2 - 4b_1b_2)^2 = 16b_1b_2(\operatorname{disc} g)^2$, where $g(X) = b_1X^2 + aX + b_2$. Although $p \nmid 2 \operatorname{disc} g$ suffices to guarantee solvability modulo p, for applying Hensel's Lemma we need to assume that $p \nmid \operatorname{disc} f$. Thus we find

Theorem 2. *The quartic $\mathcal{T}$ has a solution in $\mathbb{Q}_p$ for every prime $p \nmid 2b(a^2 - 4b_1b_2)$.*

The condition in Thm. 2 coincides with that given in [6, Chap. X, Prop. 4.9].

5. Reichardt's Counterexample to the Hasse Principle

Now let us see why Reichardt's quartic (3) violates the Hasse principle. Our arguments work for the more general quartic

$$2n^2 = X^4 - qY^4 \tag{9}$$

for primes $q \equiv 1 \bmod 8$.

Local Solutions. Multiplying through by 2 and putting $N = 2n$ we get $N^2 = 2X^4 - 2qY^4$. By Theorem 1 there are solutions to this congruence modulo every odd prime $p \neq q$, and Hensel's Lemma guarantees that we can lift these solutions to prime powers p^k.

For $p = q$, we find a p-adic solution of (3) by letting $n = X = \sqrt{2} \in \mathbb{Z}_q$ (this is Hensel's lemma at work again: from $p \equiv 1 \bmod 8$ we find that 2 is a square modulo q, and Hensel's Lemma then guarantees that 2 is a square in $\mathbb{Z}_q$) and

$Y = 0$. For $p = 2$, we can find an $x \in \mathbb{Z}_2$ such that $x^4 = q$ (solve the congruence $x^4 \equiv q \equiv 1 \bmod 8$ and lift to solutions modulo 2^k) and then put $n = 0$, $X = x$, and $Y = 1$.

Thus (9) has $\mathbb{Q}_p$-rational points for every p, and clearly has solutions in $\mathbb{R} = \mathbb{Q}_\infty$, hence has local solutions everywhere.

Global Solutions. Let $a, b, c \in \mathbb{Z}$ be pairwise relatively prime and square free. Consider the diophantine equation $aX^4 + bY^4 = cZ^2$. This equation has the trivial solution $X = Y = Z = 0$; we are interested in non-trivial solutions. We call an integral solution (X, Y, Z) *primitive* if aX, bY and cZ are pairwise relatively prime.

Lemma 5. *Let a, b, c be squarefree integers. If $aX^4 + bY^4 = cZ^2$ has a non-trivial rational solution, then it has a primitive solution.*

Proof. Suppose that $X, Y, Z \in \mathbb{Q}$ is a non-trivial rational solution. Then so is nX, nY, n^2Z where $n \in \mathbb{Z}$ is non-zero. So we can obtain a non-trivial solution in $\mathbb{Z}$.

Now let $X, Y, Z \in \mathbb{Z}$ be a non-trivial integral solution. If a prime p divides two of aX, bY, cZ then it must divide the third. Since a, b, c are pairwise relatively prime, p must divide at least two of the X, Y, and Z. This implies p^2 divides aX^4, bY^4, and cZ^2. Since a and b are squarefree, p divides X and Y. Thus p^4 divides cZ^2. Since c is squarefree, p^2 must divide Z. With $X/p, Y/p$, and Z/p^2, we get a smaller solution. Continue this process until a primitive solution is obtained. □

Now we specialize to $cZ^2 = X^4 - qY^4$ where $q \equiv 1 \bmod 8$ is a prime. Let p be an odd prime dividing Z where X, Y, Z is a primitive solution. Since the solution is primitive, X and Y are non-zero modulo p, so $(\frac{q}{p}) = 1$. 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 is the product of quadratic residues:

Lemma 6. *Suppose X, Y, Z is a primitive solution to the equation $cZ^2 = X^4 - qY^4$ where $q \equiv 1 \bmod 8$ is a prime, $c \in \mathbb{Z}$ is square free, and $q \not| c$. Then $(\frac{Z}{q}) = 1$.*

If X, Y, Z are as in the above lemma, then X and Z are non-zero modulo q since the solution is primitive. The above lemma, and the fact that $c \equiv Z^{-2}X^4 \bmod q$, gives us that c is a fourth power modulo q. To summarize:

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

Corollary 2. *Let $q \equiv 1 \bmod 8$ be a prime such that 2 is not a fourth power modulo q. Then $2Z^2 = X^4 - qY^4$ violates the Hasse principle.*

Note that $q = 17$ is such a prime since 2 is not a biquadratic residue modulo 17.

References

[1] F. Lemmermeyer, Ö. Öztürün, *Euler's Trick and Second 2-Descents*, preprint

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

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

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

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

[6] J. Silverman, *The arithmetic of elliptic curves*, Springer-Verlag 1986