EULER'S TRICK AND SECOND 2-DESCENTS

FRANZ LEMMERMEYER, ÖNCÜL ÖZTÜRÜN

1. Introduction

The first counterexamples to the Hasse principle for curves of genus 1 were constructed independently by Lind [8] and Reichardt [9]. In his survey [2, p. 206], Cassels proves Reichardt's result using a technique that "was suggested by unpublished work of Mordell".

Cassels starts with Reichardt's equation

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

which is easily seen to have nontrivial solutions in every completion $\mathbb{Q}_p$ of $\mathbb{Q}$, including $\mathbb{Q}_\infty = \mathbb{R}$ (see [1] for a proof using only elementary number theory).

Now assume that (1) has a nontrivial solution in rational numbers. Clearing denominators we may assume that X, Y, Z are nonzero integers with $\gcd(X, Y) = \gcd(X, Z) = \gcd(Y, Z) = 1$. Now we write (1) in the form

$$(5X^2 + 17Y^2)^2 - (4Z)^2 = 17(X^2 + 5Y^2)^2. \tag{2}$$

Since the left hand side is a difference of squares, it can be factored, and it is easily checked that $\gcd(5X^2 + 17Y^2 - 4Z, 5X^2 + 17Y^2 + 4Z)$ is a square or twice a square. Thus there exist nonzero integers U, V such that

$$\begin{aligned} 5X^2 + 17Y^2 \pm 4Z &= 17U^2, \\ 5X^2 + 17Y^2 \mp 4Z &= V^2, \\ X^2 + 5Y^2 &= UV, \end{aligned}$$

or

$$\begin{aligned} 5X^2 + 17Y^2 \pm 4Z &= 34U^2, \\ 5X^2 + 17Y^2 \mp 4Z &= 2V^2, \\ X^2 + 5Y^2 &= 2UV. \end{aligned}$$

Eliminating Z from the first two equations gives the systems

$$\begin{aligned} 10X^2 + 34Y^2 &= 17U^2 + V^2, \\ X^2 + 5Y^2 &= UV, \end{aligned}$$

or

$$\begin{aligned} 5X^2 + 17Y^2 &= 17U^2 + V^2, \\ X^2 + 5Y^2 &= 2UV. \end{aligned}$$

But since $(5/17) = (10/17) = -1$, none of these two systems of equations has a nonzero integral solution.

In modern language, quartics of genus 1 like (1) that have nontrivial points in every completion $\mathbb{Q}_p$ but not in $\mathbb{Q}$ represent elements of order 2 in the Tate-Shafarevich group of their Jacobian.

In his book [10, p. 317], Silverman uses this idea to study the curve $Z^2+4Y^4 = pX^4$ for primes $p = a^2+b^2 \equiv 1 \bmod 8$ and says that it is "a simple matter to verify the identity"

$$(pX^2 + 2bY^2)^2 - a^2Z^2 = p(bX^2 + 2Y^2)^2. \tag{3}$$

Where do these factorizations come from? And for which type of equations do they exist? Cassels [2] mentions that Mordell considered equations $f(x^2, y^2, z)$, where $f(X, Y, Z)$ is a quadratic form representing 0, but does not give more details.

In this article we will present a method for factoring quartics of the form $aX^4 + bY^4 = cZ^2$ with local solutions everywhere; its main idea can be traced back to Euler, and probably is very close to Mordell's unpublished work. We will show that Euler's trick can be used to construct counterexamples to the Hasse principle using only elementary number theory; in previous articles (see e.g. [5, 6, 7]), techniques from algebraic number theory were used.

We also remark that this method could very well have been used by Pépin, although there is no evidence that he did.

2. Euler's Trick

A simple way of deriving formulas giving Pythagorean triples is the following: write $x^2 + y^2 = z^2$ in the form $y^2 = z^2 - x^2 = (z + x)(z - x)$ and then use unique factorization. This method does not seem to work for simple equations like $x^2+y^2 = 2z^2$; Euler [3], however, saw that in this case multiplication by 2 saves the day because $(2z)^2 = 2x^2+2y^2 = (x+y)^2+(x-y)^2$, hence $(2z-x-y)(2z+x+y) = (x - y)^2$, and now the solution proceeds exactly as for Pythagorean triples.

Remarks in his Algebra [4, art. 181] show that Euler was aware that this trick always works for conics $aX^2 + bY^2 = cZ^2$ with a nontrivial rational point:

> So oft es aber möglich ist, [die Form $ax^2 + cy^2$ zu einem Quadrat zu machen,] kann diese Form in eine andere verwandelt werden, in welcher $a = 1$ ist. Es kann z.B. die Form $2p^2 - q^2$ zu einem Quadrat werden, sie läßt sich aber auch in solcher Art darstellen: $(2p + q)^2 - 2(p + q)^2$.

In fact, consider the conic $AX^2 + BY^2 = CZ^2$ and assume that it has a rational solution. First, multiplying through by A shows that it is sufficient to consider equations $X^2 + aY^2 = bZ^2$. Assume that (x, y, z) is a solution of this equation. Then

$$\begin{aligned}(bzZ)^2 &= bz^2X^2 + abz^2Y^2\\ &= (x^2 + ay^2)X^2 + (ax^2 + a^2y^2)Y^2\\ &= (xX + ayY)^2 + a(xY - yX)^2;\end{aligned}$$

Similarly,

$$\begin{aligned}(ayY)^2 &= aby^2Z^2 - ay^2X^2\\ &= b(bz^2 - x^2)Z^2 - (bz^2 - x^2)X^2\\ &= (xX + bzZ)^2 - b(xZ + zX)^2,\end{aligned}$$

or even

$$\begin{aligned}(xX)^2 &= bx^2Z^2 - ax^2Y^2 \\ &= b(bz^2 - ay^2)Z^2 - a(bz^2 - ay^2)Y^2 \\ &= (bzZ + ayY)^2 - ab(yZ + zY)^2.\end{aligned}$$

Euler's trick provides us with three different factorizations of the form $AB = mC^2$; we have collected them in the following table:

	A	B	C	m
I	$bzZ + ayY + xX$	$bzZ - ayY - xX$	$xY - yX$	a
II	$bzZ + ayY + xX$	$bzZ - ayY + xX$	$xZ + zX$	b
III	$bzZ + ayY + xX$	$bzZ + ayY - xX$	$yZ + zY$	ab

TABLE 1. Factorizations $AB = mC^2$ derived from Euler's Trick

In Euler's example $y^2 + z^2 = 2x^2$ we have $(x, zy, z, a, b) = (1, 1, 1, 1, 2)$, and the third factorization gives $z^2 = (2x + y)^2 - 2(x + y)^2$.

3. Bounding the GCD

For applying unique factorization we have to determine the greatest common divisor of the factors A and B in Table 2. First observe that we may assume that a and b are squarefree since we can subsume squares into Y^2 or Z^2.

Lemma 1. *Assume that a and b are squarefree. If $\mathcal{C} : X^2 + aY^2 = bZ^2$ has a nontrivial solution (x, y, z), then it has an integral point (X, Y, Z) with $\gcd(X, Y) = \gcd(X, Z) = \gcd(Y, Z) = 1$.*

Proof. Multiplying through by the square of the gcd's of a nontrivial solution we may clearly assume that there is an integral solution. Put $d = \gcd(X, Y)$. Then $d^2 \mid bZ^2$, and since b is squarefree, we easily conclude that $d \mid Z$. □

For bounding $d = \gcd(A, B)$ we need to make several assumptions: we will assume that $\gcd(Y, Z) = 1$, which we are allowed to do by Lemma 1; we will call a solution (X, Y, Z) primitive if $\gcd(X, Y) = \gcd(Y, Z) = \gcd(Z, X) = 1$. By the same reason we may assume that (x, y, z) is primitive. The gcd of the two factors is then described by the following

Theorem 2. *Assume that (x, y, z) is a primitive solution of $\mathcal{C} : X^2 + aY^2 = bZ^2$, where a and b are coprime and squarefree integers. Then for any primitive solution (X, Y, Z) of $\mathcal{C}$, we have $\gcd(A, B) = \delta u^2$, where δ and u are integers satisfy the following conditions:*

I	$\delta \mid 2b$	$u \mid \gcd(z, Z)$
II	$\delta \mid 2a$	$u \mid \gcd(y, Y)$
III	$\delta \mid 2$	$u \mid \gcd(x, X)$

Proof. The proofs for the three cases are completely analogous; thus it will be sufficient to give the proof only for case I.

In this case we clearly have

$$\begin{aligned} d \mid (A+B) &= 2bzZ, \\ d \mid (A-B) &= 2(ayY+xX), \\ d^2 \mid AB &= a(yX-xY)^2. \end{aligned}$$

Since a is squarefree, the last relation shows that $d^2 \mid (yX-xY)^2$, hence $d \mid (yX-xY)$. Now $d \mid 2x(ayY+xX)$ and $d \mid 2ay(yX-xY)$ implies $d \mid 2(x^2+ay^2)X = 2bz^2X$. Together with $d \mid 2bzZ$ this implies $d \mid 2\gcd(bz^2X, bzZ) = 2bz\gcd(z,Z) \mid 2bz^2$.

From $bZ^2 = X^2+aY^2$ we get $bx^2Z^2 = x^2X^2+ax^2Y^2 = (bz^2-ay^2)X^2+ax^2Y^2$, hence

$$b(x^2Z^2 - z^2X^2) = a(xY-yX)(xY+yX). \tag{4}$$

Multiplying through by 2 we see that $d \mid 2bx^2Z^2$. Thus $d \mid \gcd(2bz^2, 2bx^2Z^2) = 2b\gcd(z^2, x^2Z^2) = 2b(z,Z)^2$.

We now claim that d is a divisor of $2b$ times a square. We know that $d \mid 2b\gcd(z,Z)^2$. Now write $\gcd(d,z,Z) = 2^j\beta u$, where u is the maximal odd divisor of d coprime to b. From $u^2 \mid z^2$, $u^2 \mid Z^2$ and (4) we get $u^2 \mid a(xY-yX)(xY+yX)$.

Next observe that $\gcd(z,Z)$ is coprime to a: in fact, if q is a prime dividing $\gcd(a,z)$, then $q \mid x^2$, hence $q \mid z$, and this contradicts the assumption that $\gcd(x,z) = 1$. Thus we have $u^2 \mid (xY-yX)(xY+yX)$.

Now we claim that no prime $q \mid u$ divides the first factor. Otherwise q would divide both factors, hence xY and yX. Since $q \mid z$ we have $q \nmid xy$, hence $q \mid X$ and $q \mid Y$: contradiction. This implies that $u^2 \mid (zY+yZ)$.

But then $u^2 \mid d \mid 2\gcd(d,x,X)^2 = 2^{j+1}\beta u^2$. This implies the claim. □

The bounds for the gcd's given at the end of Theorem 2 are best possible: they are attained for $(X,Y,Z) = (x,y,-z)$.

4. Unique Factorization

Consider the first factorization $AB = mC^2$, where $A = bzZ+ayY+xX$, $B = bzZ-ayY-xX$, $C = xY-yX$, and $m = a$; then $\gcd(A,B) = \beta u^2$ for some $\beta \mid 2b$. Unique Factorization then gives the system of equations

$$\begin{aligned} bzZ+ayY+xX &= \alpha\beta r^2, \\ bzZ-ayY-xX &= \alpha'\beta s^2, \\ xY-yX &= \beta rs, \end{aligned}$$

where $\alpha\alpha' = a$.

Let us now consider Pépin's examples. His quartics all have the form $pX^4 - mY^4 = Z^2$; the rational solution $(\alpha, b, \alpha^2a+\beta b)$ of the underlying conic $x^2+my^2 = pz^2$ gives rise to the Euler factorizations

$$=$$

Eliminating Z gives

$$\begin{aligned} 2(ayY+xX) &= \beta(\alpha r^2 - \alpha' s^2), \\ xY-yX &= \beta rs, \end{aligned}$$

Eliminating X finally gives the equation

$$2bz^2Y = \beta(\alpha r^2 - \alpha' s^2 - 2xrs)$$

5. Silverman's example

We have $X^2+4Y^4 = pZ^4$. The conic underlying Silverman's example is $\xi^2+\eta^2 = p\zeta^2$, where we have set $\xi = X$, $\eta = 2Y^2$ and $\zeta = Z^2$. Here $a = 1$, $b = p$, and with $p = c^2 + d^2$ we get the solution $(x, y, z) = (c, d, 1)$. Euler's factorizations are given by

$$\begin{aligned}(p\zeta + c\xi + d\eta)(p\zeta - c\xi - d\eta) &= (d\xi - c\eta)^2,\\ (c\xi + p\zeta + d\eta)(c\xi + p\zeta - d\eta) &= p(c\zeta + \xi)^2,\\ (p\zeta + d\eta + c\xi)(p\zeta + d\eta - c\xi) &= p(d\zeta + \eta)^2.\end{aligned}$$

Introducing the original variables again, the third factorization gives

$$p(dZ^2 + 2Y^2)^2 = (pZ^2 + 2dY^2 + cX)(pZ^2 + 2dY^2 - cX).$$

Assuming that (X, Y, Z) is primitive, Theorem 2 tells us that $\gcd(pZ^2 + 2dY^2 + cX, pZ^2+2dY^2-cX) = 2^je^2$ for some odd integer e (note that $z = 1$ here). Unique factorization then implies (replacing Z by $-Z$ if necessary)

$$\begin{aligned}pZ^2 + 2dY^2 + cX &= \delta pu^2,\\ pZ^2 + 2dY^2 - cX &= \delta v^2,\\ dZ^2 + 2Y^2 &= \delta uv,\end{aligned}$$

where $\delta \in \{1, 2\}$. Eliminating X yields the pair of equations

$$\begin{aligned}2pZ^2 + 4dY^2 &= \delta(v^2 + pu^2),\\ dZ^2 + 2Y^2 &= \delta uv.\end{aligned}$$

Now we distinguish two cases:

(1) $\delta = 1$: reducing the equations modulo 8 and using $4 \mid d$ we find $2Z^2 \equiv u^2 + v^2 \bmod 8$. This implies $u \equiv v \bmod 2$, and the second equation shows that uv is even. Thus both u and v are even, and then the first equation shows that $2 \mid Z$, the second that $2 \mid Y$: contradiction.

(2) $\delta = 2$: then we find $Z^2 \equiv u^2 + v^2 \bmod 8$. If Z is even, then both u and v must be even, and then the second equation implies that Y is also even, which again contradicts $(Y, Z) = 1$. Thus Z is odd, hence one of u, v is odd and the other is divisible by 4 (because of $v^2 \equiv X^2 - u^2 \equiv 0 \bmod 8$). But then Y must be even, and the second equation gives $d \equiv 0 \bmod 8$.

We have proved:

Theorem 3. *If the diophantine equation $X^2 + 4Y^4 = pZ^4$, where $p = c^2 + d^2 \equiv 1 \bmod 8$ is a prime, has a nontrivial solution, then $d \equiv 0 \bmod 8$.*

6. Pépin's Results

In [5], the theorem below was proved (under the additional assumption that α be prime) using genus theory; here we will show how Euler's trick can be used to give an elementary proof.

Theorem 4. *Let $a, b, \alpha, \beta, \gamma$ be integers such that $p = \alpha^2a^2 + 2\beta ab + \gamma b^2$ is an odd prime. Then the conic $X^2 + mY^2 = pZ^2$, where $m = \alpha^2\gamma - \beta^2$, has the integral point $(\alpha^2a + \beta b, b, \alpha)$.*

If, in addition, $m \equiv 1 \bmod 8$ is a prime and $\alpha \equiv 3 \bmod 4$, then the equation

$$px^4 - my^2 = z^2 \tag{5}$$

does not have any nontrivial rational solutions.

6.1. **Preliminaries.** We now prove a few simple properties that we will use later on:

If we put $z = X$, $y = Y$ and $x^2 = Z$, then (5) becomes

$$X^2 + mY^2 = pZ^2. \tag{6}$$

Lemma 5. *If $m \equiv 1 \bmod 4$, then any nontrivial solution of (6) with $\gcd(X, Y) = 1$ satisfies $Z \equiv 1 \bmod 2$, and we have $p \equiv 1 \bmod 4$.*

Proof. If $2 \mid Z$, then $X \equiv Y \bmod 2$, and since $\gcd(X, Y) = 1$ both X and Y are both odd. But then we find the contradiction $0 \equiv pZ^2 \equiv X^2 + mY^2 \equiv 2 \bmod 4$.

Now $px^4 \equiv my^2 + z^2 \equiv y^2 + z^2 \bmod 4$ implies $p \equiv 1 \bmod 4$. □

6.2. **Euler's Trick.** We start with the factorization

$$m((\alpha^2a + \beta b)Y - bX)^2 = (p\alpha^2Z)^2 - ((\alpha^2a + \beta b)X + mbY)^2. \tag{7}$$

Now we put

$$\begin{aligned} A &= p\alpha Z - X(\alpha^2a + \beta b) - mbY, \\ B &= p\alpha Z + X(\alpha^2a + \beta b) + mbY, \\ C &= (\alpha^2a + \beta b)Y - bX \end{aligned}$$

and get $AB = mC^2$.

6.3. **Unique Factorization.** Since $a = m$ and $b = p$, Theorem 2 shows $\gcd(A, B) = \delta u^2$ for some integer $\delta \mid 2p$.

Since $AB = mC^2$ for a prime m and $\gcd(A, B) = \delta u^2$, there exist $r, s \in \mathbb{Z}$ such that $A = \delta r^2, B = \delta ms^2$ or $A = \delta mr^2$ and $B = \delta s^2$. Since changing the signs of X and Y corresponds to switching A and B, we may assume that we have $A = \delta r^2$ and $B = \delta ms^2$.

Note that since $A + B = 2p\alpha Z > 0$ (since Z is a square) and $AB = mC^2 > 0$, we must have $A, B > 0$. Now consider the following cases:

(1) $\delta \equiv 1 \bmod 4$, i.e., $\delta \in \{1, p\}$. Here $2p\alpha Z = A+B = \delta(r^2+ms^2)$. Now r and s must have the same parity; if they are both even, then Z is divisible by 4; therefore we may divide the equation $2p\alpha Z = A+B = \delta(r^2+ms^2)$ through by powers of 2 until both r and s are odd. But then $p\alpha Z \equiv 1 \bmod 4$, hence $Z \equiv 3 \bmod 4$, hence Z cannot be a square.

(2) $\delta \equiv 2 \bmod 4$, i.e., $\delta \in \{2, 2p\}$. Here $p\alpha Z = \frac{1}{2}(A + B) = \delta'(r^2 + ms^2)$ with $\delta' \in \{1, p\}$. As above we get $Z \equiv 3 \bmod 4$, and again Z cannot be a square.

The only place where we have used the primality of m was in the last subsection. If $m \equiv 1 \bmod 8$ is a product of primes $\equiv 1 \bmod 4$, then we get the equations $A = \delta\mu r^2$, $B = \delta\nu s^2$ with $\mu\nu = m$. Again we have to consider the following cases:

(1) $\delta \equiv 1 \bmod 4$, i.e., $\delta \in \{1, p\}$. Then $2p\alpha Z = A + B = \delta(\mu r^2 + \nu s^2)$; now r and s must have the same parity, and since we know that their gcd is odd, we must have $r \equiv s \equiv 1 \bmod 2$. This implies $p\alpha Z \equiv \frac{1}{2}\mu + \nu \equiv 1 \bmod 4$ (note that $\mu, \nu \equiv 1 \bmod 4$ and $\mu\nu \equiv 1 \bmod 8$ imply that $\mu + \nu \equiv 2 \bmod 8$), hence $Z \equiv 3 \bmod 4$, and Z cannot be a square.

(2) $\delta \equiv 2 \bmod 4$, i.e., $\delta \in \{2, 2p\}$. Here $p\alpha Z = \frac{1}{2}(A + B) = \delta'(\mu r^2 + \nu s^2)$ with $\delta' \in \{1, p\}$. As above we get $Z \equiv 3 \bmod 4$, and again Z cannot be a square.

The following examples were claims made by Pépin:

α	β	γ	m	p
3	1	2	17	$9a^2 + 2ab + 2b^2$
3	2	5	41	$9a^2 + 4ab + 5b^2$
3	5	10	65	$9a^2 + 10ab + 10b^2$
3	7	14	77	$9a^2 + 14ab + 14b^2$
7	1	2	97	$49a^2 + 2ab + 2b^2$

The example $m = 77$ is not covered by Theorem 4. We leave it to the reader to prove the following result:

Proposition 6. *Assume that $m = pq \equiv 1 \bmod 8$ for primes $p \equiv 7 \bmod 8$ and $q \equiv 3 \bmod 8$ such that $(\alpha/p) = -1$. Then the equation does not have a nontrivial rational solution.*

References

[1] W. Aitken, F. Lemmermeyer, *Quartics of genus* 1, preprint

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

[3] L. Euler, *Theorematum quorundam arithmeticorum demonstrationes*, Comm. Acad. Sci. Petrop. **10** (1738) 1747, 125–146; Opera Omnia Ser. I vol. II, Commentationes Arithmeticae, 38–58

[4] L. Euler, *Vollständige Anleitung zur Algebra*, Petersburg 1770; Russ. Transl. Petersburg 1768/69

[5] F. Lemmermeyer, *A note on Pépin's counter examples to the Hasse principle for curves of genus* 1, Abh. Math. Sem. Hamburg **69** (1999), 335–345

[6] F. Lemmermeyer, *On Tate-Shafarevich groups of some elliptic curves*, Proc. Conf. Graz 1998, (2000), 277–291

[7] F. Lemmermeyer, *Some families of non-congruent numbers*, Acta Arith. **110** (2003), 15–36

[8] C.E. Lind, *Untersuchungen über die rationalen Punkte der ebenen kubischen Kurven vom Geschlecht eins*, Ph.D. thesis Uppsala 1940

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

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