EULER'S TRICK AND SECOND 2-DESCENTS

FRANZ LEMMERMEYER, ÖNCÜL ÖZTÜRÜN

Abstract. In this article we present an elementary method for investigating the solvability of certain quartic diophantine equations (in modern language: we show how to perform the second 2-descent on certain elliptic curves using only the arithmetic of integers). Our method is based on an idea of Euler and seems to be related to unpublished work of Mordell.

1. Hasse's Local-Global Principle

One of the simplest examples of the Local-Global Principle is the fact that equations of the form $ax^2 + by^2 = cz^2$ (in geometric language, these are conics in the projective plane) with coefficients $a, b, c \in \mathbb{Z}$ (or, more generally, in $\mathbb{Q}$) have a nontrivial solution in $\mathbb{Q}$ if and only if they have a nontrivial solution in every completion $\mathbb{Q}_p$, i.e., if and only if they have a solution in the reals $\mathbb{R} = \mathbb{Q}_\infty$ and modulo every $m \ge 1$ (see [9] for an elementary introduction to p-adic numbers).

More generally, a property P is said to satisfy the Local-Global Principle if the following statement holds: P is true in $\mathbb{Q}$ if and only if the corresponding statement holds in every completion of $\mathbb{Q}$; more generally, $\mathbb{Q}$ may be replaced by any global field, i.e., a number field or a finite extension of $\mathbb{F}_p(X)$. A trivial example of a property for which the Local-Global Principle holds is the fact that a nonzero rational number is a square in $\mathbb{Q}$ if and only if it is a square in every $\mathbb{Q}_p$.

2. Reichardt's Example

The first counterexamples to the Hasse principle for curves of genus 1 were constructed independently by Lind [8] and Reichardt [10]. In fact, the curve

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

of genus 1 is such a counterexample. For proving this we have to show the following claims:

1. (1) has nontrivial points in every completion $\mathbb{Q}_p$;
2. (1) does not have a nontrivial rational point.

The first claim is a special case of a quite general theorem of F.K.Schmidt (proved using the theorem of Riemann-Roch and zeta functions for function fields) according to which every curve of genus 1 defined over a finite field has at least one point; for (1), these points defined over $\mathbb{F}_p$ can be lifted to points defined over $\mathbb{Z}_p$ using Hensel's Lemma.

A more elementary proof uses Gauss sums to count the number of points of (1) over finite fields. Finally, a completely elementary argument is given in [1].

The second claim can easily be proved using a slightly tricky calcluation involving the quadratic reciprocity law. In his survey [2, p. 206] on curves of genus 1, Cassels

proves this result using a technique that he says "was suggested by unpublished work of Mordell".

Cassels assumes 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, as Cassels says, "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 [11, p. 317], Silverman uses this idea to study the curve $Z^2 + 4Y^4 = pX^4$ for primes $p = c^2 + d^2 \equiv 1 \bmod 8$ and says that it is "a simple matter to verify the identity"

$$(pX^2 + 2dY^2)^2 - c^2Z^2 = p(dX^2 + 2Y^2)^2. \tag{3}$$

Where does this factorization come from? And for which type of equations do such factorizations 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 an elementary 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 quite likely is closely related to Mordell's unpublished work referred to above. 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.

Here is the broad outline: we start with a quartic of type $aX^4 + bY^4 = cZ^2$ with nontrivial solutions everywhere locally. Then the underlying conic $f(x, y, z) = ax^2 + by^2 - cz^2 = 0$ has local solutions everywhere, hence has a nontrivial rational point (ξ, η, ζ). The existence of this point implies, by "Euler's trick", that the conic can be factored in the form $f(x, y, z) = AB - mC^2$ for some $m \in \mathbb{Z}$ depending on a, b, c and ξ, η, ζ, where A, B, C are linear forms. By carefully examining the possibilities for the greatest common divisor $\gcd(A, B)$ of the factors on the left hand side and invoking unique factorization we are then able to derive a finite list auxiliary equations; if we can show that none of these have solutions with x or y a square, then we will have proved that the original quartic does not have any nontrivial rational solutions.

We also remark that this method could very well have been used by Pépin (see [5]), although there is no evidence that he did.

3. Second 2-Descents and Tate-Shafarevich Groups

Although the statements and the proofs of the results of this article are completely elementary, the big picture involves some more advanced notions from the theory of elliptic curves. It is well known that the 2-descent on elliptic curves $y^2 = (x - a)(x - b)(x - c)$ with three rational points $(a, 0)$, $(b, 0)$, $(c, 0)$ of order 2 can be performed only using elementary number theory. If an elliptic curve $E : y^2 = x(x^2 + ax + b)$ has only one rational point $(0, 0)$ of order 2, then multiplication by 2 gives an isogeny $E \longrightarrow E$ that can be factored into two isogenies $\phi : E \longrightarrow E'$ and $\phi' : E' \longrightarrow E$ of degree 2. The first descent via ϕ leads to a set of auxiliary quartics

$$\mathcal{T}(b_1) : N^2 = b_1 M^4 + aM^2 e^2 + b_2 e^4, \quad b_1 b_2 = b \tag{4}$$

with the property that each rational point on E gives rise to a rational point on one of the finitely many curves $\mathcal{T}(b_1)$, and that conversely every rational point on one of the $\mathcal{T}(b_1)$ provides us with a rational point on E. Thus for showing that $E(\mathbb{Q})$ is trivial (i.e., only contains the point at infinity) it is sufficient to check that none of the $\mathcal{T}(b_1)$ have a rational point. This often can be achieved by showing that none of the $\mathcal{T}(b_1)$ have solutions in every $\mathbb{Q}_p$. This can be done using elementary number theory: see [1].

Occasionally, however, it will happen that some $\mathcal{T}(b_1)$ is everywhere locally solvable and still has no rational point. In such a case, $\mathcal{T}(b_1)$ represents an element of order 2 in the Tate-Shafarevich group $Ш(E)$ of E over $\mathbb{Q}$.

Checking that a given $\mathcal{T}(b_1)$ is everywhere locally solvable is easy; making sure that there is no rational point on $\mathcal{T}(b_1)$ is usually done by a second 2-descent. In this article we will explain how to do this by generalizing the examples of Cassels and Silverman presented above.

4. Euler's Trick

One way of deriving formulas giving Pythagorean triples is the following: write the Pythagorean equation $x^2 + y^2 = z^2$ 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

$$x^2 + y^2 = 2z^2; \tag{5}$$

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 $ax^2 + cy^2 = z^2$ 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: $(2p+q)^2 - 2(p+q)^2$.[1]

Euler's claim can be justified quite easily. In fact, consider the conic $ax^2 + by^2 = cz^2$. Multiplying through by a shows that it is sufficient to consider equations of the form $x^2 + ay^2 = bz^2$. Assume now that (ξ, η, ζ) is a nontrivial solution of this equation (such solutions exist by the Local-Global Principle if and only if the conic has nontrivial points in every completion of $\mathbb{Q}$). Then multiplying $bz^2 = x^2 + ay^2$ through by $b\zeta^2$ gives

$$\begin{aligned}(b\zeta z)^2 &= b\zeta^2 x^2 + ab\zeta^2 y^2 \\ &= (\xi^2 + a\eta^2)x^2 + (a\xi^2 + a^2\eta^2)y^2 \\ &= (\xi x + a\eta y)^2 + a(\xi y - \eta x)^2.\end{aligned}$$

Similarly,

$$\begin{aligned}(a\eta Y)^2 &= ab\eta^2 z^2 - a\eta^2 x^2 \\ &= b(b\zeta^2 - \xi^2)z^2 - (b\zeta^2 - \xi^2)x^2 \\ &= (\xi x + b\zeta z)^2 - b(\xi z + \zeta x)^2,\end{aligned}$$

or

$$\begin{aligned}(\xi X)^2 &= b\xi^2 z^2 - a\xi^2 y^2 \\ &= b(b\zeta^2 - a\eta^2)z^2 - a(b\zeta^2 - a\eta^2)y^2 \\ &= (b\zeta z + a\eta y)^2 - ab(\eta z + \zeta y)^2.\end{aligned}$$

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

In Euler's example (5) we have $(\xi, \eta, \zeta, a, b) = (1, 1, 1, 1, 2)$, and the third factorization gives $z^2 = (2x+y)^2 - 2(x+y)^2$, which is the factorization that Euler presented in the quote given above.

---

[1] Whenever it is possible [to make the form $ax^2 + cy^2$ into a square,] this form can be transformed into one in which $a = 1$. For example, we can make $2p^2 - q^2$ into a square, and it can be represented in the following form: $(2p+q)^2 - 2(p+q)^2$.

	A	B	C	m
I	$b\zeta z + a\eta y + \xi x$	$b\zeta z - a\eta y - \xi x$	$\xi y - \eta x$	a
II	$b\zeta z + a\eta y + \xi x$	$b\zeta z - a\eta y + \xi x$	$\xi z + \zeta x$	b
III	$b\zeta z + a\eta y + \xi x$	$b\zeta z + a\eta y - \xi x$	$\eta z + \zeta y$	ab

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

5. Bounding the GCD

For applying unique factorization we have to determine the greatest common divisor of the factors A and B in Table 1. First observe that we may assume that a and b are squarefree since we can subsume squares into y^2 or z^2. As a warning we remark that this cannot be done for the original quartic!

Lemma 1. *Assume that a and b are squarefree. If $\mathcal{C} : x^2 + ay^2 = bz^2$ has a nontrivial solution (ξ', η', ζ'), then it has an integral point (ξ, η, ζ) with $\gcd(\xi, \eta) = \gcd(\xi, \zeta) = \gcd(\eta, \zeta) = 1$.*

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 $d = \gcd(\xi, y)$. Then $d^2 \mid b\zeta^2$, and since b is squarefree, we easily conclude that $d \mid \zeta$. □

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 $\gcd(x, y) = \gcd(y, z) = \gcd(z, x) = 1$. In particular we may assume that (ξ, η, ζ) is primitive. The gcd of the two factors is then described by the following

Theorem 2. *Assume that (ξ, η, ζ) 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 $\delta \mid \frac{2ab}{m}$.*

More exactly, δ and u are integers satisfying the following conditions:

case	*bound for δ*	*bound for u*
I	$\delta \mid 2b$	$u \mid \gcd(\zeta, z)$
II	$\delta \mid 2a$	$u \mid \gcd(\eta, y)$
III	$\delta \mid 2$	$u \mid \gcd(\xi, x)$

For the proof we will use without comment several trivial properties of the gcd; in the following, a, b, d, m, n denote integers:

1. $\gcd(a, b) \mid \gcd(ma + nb)$;
2. $d \mid a$ and $d \mid b$ imply $d \mid \gcd(a, b)$;
3. $d^2 \mid am^2$ for squarefree a implies $d \mid m$;
4. $d \mid A + B$ and $d^2 \mid AB$ imply $d \mid A - B$.

Proof of Thm. 2. 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, recall that

$$A = b\zeta z + a\eta y + \xi x$$
$$B = b\zeta z - a\eta y - \xi x$$
$$C = \xi y - \eta x$$

Here is what we will do: let $d = \gcd(A, B)$ and write $\gcd(\zeta, z) = 2^j u$ for some odd integer u. Then we will prove that

$$d \mid 2^{j+1} b u^2, \tag{6}$$

$$u^2 \mid d; \tag{7}$$

these relations clearly imply our claims.

Proof of (6). We clearly have

$$d \mid (A + B) = 2b\zeta z, \tag{8}$$

$$d \mid (A - B) = 2(a\eta y + \xi x), \tag{9}$$

$$d^2 \mid AB = a(\eta x - \xi y)^2. \tag{10}$$

Since a is squarefree, the last relation implies

$$d \mid (\eta x - \xi y). \tag{11}$$

Multiplying (9) and (10) through by ξ and 2η, respectively, gives $d \mid 2\xi(a\eta y + \xi x)$ and $d \mid 2a\eta(\eta x - \xi y)$. Adding these relations shows that $d \mid 2(\xi^2 + a\eta^2)x = 2b\zeta^2 x$. Together with (8) this implies that $d \mid 2\gcd(b\zeta^2 x, b\zeta z) = 2b\zeta \gcd(\zeta, z) \mid 2b\zeta^2$:

$$d \mid 2b\zeta^2. \tag{12}$$

From $bz^2 = x^2 + ay^2$ we get $b\xi^2 z^2 = \xi^2 x^2 + a\xi^2 y^2 = (b\zeta^2 - a\eta^2)x^2 + a\xi^2 y^2$, hence

$$b(\xi^2 z^2 - \zeta^2 x^2) = a(\xi y - \eta x)(\xi y + \eta x). \tag{13}$$

Multiplying through by 2 we see that d divides the right hand side because of (11), and the term $2b\zeta^2 x^2$ on the left hand side decause of (12). Thus $d \mid 2b\xi^2 z^2$. This relation and (12) now imply $d \mid \gcd(2b\zeta^2, 2b\xi^2 z^2) = 2b\gcd(\zeta^2, \xi^2 z^2) = 2b\gcd(\zeta, z)^2$:

$$d \mid 2b\gcd(\zeta, z)^2. \tag{14}$$

Proof of (7). From $u^2 \mid \zeta^2$, $u^2 \mid z^2$ and (13) we get

$$u^2 \mid a(\xi y - \eta x)(\xi y + \eta x).$$

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

Now we claim that no prime $q \mid u$ divides the second factor. Otherwise q would divide both factors, hence ξy and ηx. Since $q \mid \zeta$ we have $q \nmid \xi\eta$, hence $q \mid x$ and $q \mid y$: contradiction. This implies that $u^2 \mid (\xi y - \eta x)$.

But then $u^2 \mid A + B$ and $u^2 \mid AB$, hence $u^2 \mid A - B$ and therefore $u^2 \mid A$ and $u^2 \mid B$. But then $u^2 \mid d$ as claimed. □

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

6. Silverman's example

Let $p = c^2 + d^2 \equiv 1 \bmod 8$ be a prime, and consider the quartic $X^2 + 4Y^4 = pZ^4$. Its underlying conic has equation $\xi^2 + \eta^2 = p\zeta^2$, 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

$$\gcd(pZ^2 + 2dY^2 + cX, pZ^2 + 2dY^2 - cX) = 2^j e^2$$

for some odd integer e (note that $z = 1$ here).[2] Unique factorization then implies (replacing Z by $-Z$ if necessary)

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

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. *Let $p = c^2 + d^2 \equiv 1 \bmod 8$ be prime. If the diophantine equation $X^2 + 4Y^4 = pZ^4$ has a nontrivial solution in integers, then $d \equiv 0 \bmod 8$.*

[2] Silverman claims that "it is not difficult to check" that the gcd is a square or twice a square, and that it equals a power of 2 times $\gcd(X, c)^2$. Actually, the gcd equals $2^j u^2$ for some $u \mid \gcd(X, c)$.

7. 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, $\alpha \equiv 3 \bmod 4$, and if $m \equiv 1 \bmod 8$ is a product of primes $\equiv 1 \bmod 4$, then the equation

$$pX^4 - mY^2 = Z^2 \tag{15}$$

does not have any nontrivial rational solutions.

7.1. **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 (15) becomes

$$x^2 + my^2 = pz^2. \tag{16}$$

Lemma 5. *If $m \equiv 1 \bmod 4$, then any nontrivial solution of (16) 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 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 $p \equiv 1 \bmod 4$. □

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

$$m((\alpha^2a + \beta b)y - bx)^2 = (p\alpha^2z)^2 - ((\alpha^2a + \beta b)x + mby)^2. \tag{17}$$

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 $AB = mC^2$.

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

Note that since $A+B = 2p\alpha z > 0$ (since $z = X^2$ is a square) and $AB = mC^2 > 0$, we must have $A, B > 0$. Since $m \equiv 1 \bmod 8$ is a product of primes $\equiv 1 \bmod 4$, we get the equations $A = \delta\mu r^2$, $B = \delta\nu s^2$ with $\mu\nu = m$. Now 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.

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	$9a^2+10ab+10b^2$
7	1	2	97	$49a^2+2ab+2b^2$

TABLE 2. Some of Pépin's Results

The following examples were claims made by Pépin:

Let us now check the local solvability of (15). By a standard result (see [1] for an elementary proof), we only have to check solvability in $\mathbb{Q}_q$ for primes $q \mid 2pm$.

Note that the solvability of $x^2+my^2=pz^2$ implies that $(p/q)=1$ for every prime $q \mid m$. Thus putting $(X,Y,Z)=(1,0,\sqrt{p}\,)$ is a nontrivial solution of (15) in $\mathbb{Q}_q$ for all $q \mid m$.

Moreover, the fact that $p \equiv 1 \bmod 4$ and $(p/q)=1$ for all $q \mid m$ implies $(-m/p)=+1$, hence $(X,Y,Z)=(0,1,\sqrt{-m}\,)$ is a nontrivial solution of (15) in $\mathbb{Q}_p$.

It remains to check solvability in $\mathbb{Q}_2$. A necessary and sufficient condition is the solvability of $Z^2 \equiv pX^4 \bmod 8$, hence (15) has solutions in $\mathbb{Q}_2$ if and only if $p \equiv 1 \bmod 8$.

Theorem 6. *Pépin's claims listed in Table 2 above produce counterexamples to the Hasse principle for those primes p for which $4 \mid b$, or $a \equiv 3 \bmod 4$ and $2 \nmid b$.*

REFERENCES

[1] W. Aitken, F. Lemmermeyer, *Simple counterexamples to the Local-Global Principle*, 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] Matematik Dünyasi, 2004

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

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