GENUS 1 PRELIMINARIES

SAMIR SIKSEK

Abstract. These are notes and exercises for the first lecture at the Stieltjes and Diamant Onderwijsweek Solvability of Diophantine Equations workshop, Leiden, 2007. All the material is perfectly standard.

Contents

1. Weierstrass Elliptic Curves

It is expected that you have previously met elliptic curves and are familiar with the group law and with the Mordell-Weil Theorem. The purpose of these notes is to acquaint you with some of the practical aspects of the arithmetic of curves of genus 1.

Let K be a number field, and let $\mathcal{O}_K$ is its ring of integers. A Weierstrass elliptic curve E over K has the model

$$E \ : \quad y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6 \tag{1}$$

where the coefficients $a_i \in K$ and the discriminant is non-zero. The discriminant is a complicated expression in the coefficients, but saying that it is non-zero is equivalent to saying that the curve E is non-singular. The model shown here for E is an affine model, but we never forget that E has point at infinity, which happens to be the zero of the group law defined on E.

We usually prefer to work with an integral model for E where $a_i \in \mathcal{O}_K$; this can be obtained by appropriate scaling. We denote the set of K-rational points on E by $E(K)$; this is the set of pairs $(a, b) \in K^2$ that satisfy the equation for E together with the point at infinity.

Theorem 1. *(The Mordell-Weil Theorem) Let E be an elliptic curve over a number field K. The abelian group $E(K)$ is finitely generated.*

Date: May 2, 2007.

This means that $E(K) \cong T \times \mathbb{Z}^r$ where $T = \mathrm{Tors}(E(K))$ is the torsion subgroup of $E(K)$ (the subgroup of points of finite order) and r is a non-negative integer, called the rank of E. The torsion subgroup is finite and computable. We can rephrase the Mordell-Weil Theorem as follows: there exists $P_1, \cdots, P_r \in E(K)$ such that every point $P \in E(K)$ is uniquely expressible as

$$P = P_0 + n_1 P_1 + n_2 P_2 + \cdots + n_r P_r$$

where $P_0 \in T$ and $n_i \in \mathbb{Z}$. The set $\{P_1, \ldots, P_r\}$ is called a Mordell-Weil basis for $E(K)$. One of the major open questions is to give an algorithm that is guaranteed to compute a basis for elliptic curves over number fields. No such algorithm is known; we do however have a descent strategy which often succeeds in computing such a basis.

Example 1.1. Let E be the elliptic curve over the rationals given by

$$E \ : \quad y^2 + y = x^3 - x^2 - 7x + 10.$$

Carrying out a descent by hand to compute a Mordell-Weil basis can be an unpleasant business. There several computer packages that will do this for us. Any of these would tell us that the torsion subgroup $\mathrm{Tors}(E(K)) = \{O\}$, the rank is 1 and we can take $Q = (4, 5)$ as a basis element. Thus every $P \in E(\mathbb{Q})$ can be written as $P = nQ$ for a unique $n \in \mathbb{Z}$.

Let us see how to do this in the package MAGMA. You must specify the curve using its coefficients a_1, a_2, a_3, a_4, a_6 (compare the equation for E with (1) to know which is which. In MAGMA to specify E we type:

```
> E:=EllipticCurve([0,-1,1,-7,10]);
```

To check that we have done this correctly, we ask for E:

```
> E;
Elliptic Curve defined by y^2 + y = x^3 - x^2 - 7*x + 10 over Rational Field
```

Now let us ask for the Mordell-Weil group:

```
> MordellWeilGroup(E);
Abelian Group isomorphic to Z
Defined on 1 generator (free)
```

This is tell us that there is trivial torsion and the rank is 1. But what is a basis:

```
> Generators(E);
[ (4 : 5 : 1) ]
```

Notice that the generating point is given in projective coordinates.

2. Curves of Genus 1

We shall not define the genus of a curve, but we will see a few families of curves of genus 1 and specify a few things that you need to know about curves of genus 1. An elliptic curve over a field K is often defined as a curve of genus 1 over K with a K-rational point P_0.

Theorem 2. *If C is a curve of genus 1 and $P_0 \in C(K)$ then there a Weierstrass model E defined over K (given by a Weierstrass equation (1)), and a birational map*

$$\phi : C \to E$$

defined over K such that $\phi(P_0) = O$ (the point at infinity on E).

You should be familiar with several families of curves of genus 1:

(I) Curves of the form

$$y^2 = a_4x^4 + a_3x^3 + a_2x^2 + a_1x + a_0 \tag{2}$$

where $a_4 \neq 0$ and the polynomial on the right-hand side has distinct roots; i.e. the discriminant is non-zero. Working with such curves, it is important to realise that there are two points at infinity. Let $x = X/Z$ and $y = Y/Z^2$. Clearing denominators we obtain

$$Y^2 = a_4X^4 + a_3X^3Z + a_2X^2Z^2 + a_1XZ^3 + a_0Z^4. \tag{3}$$

This is a curve in weighted projective space with weights 1, 2, 1 on the variables X, Y, Z. A point (x, y) on the affine model (2) corresponds to the point $[X : Y : Z] = (x : y : 1)$ on the weighted projective model. The two points at infinity are $[1 : \pm\sqrt{a_4} : 0]$. Thus the points at infinity are rational if and only if a_4 is a square.

(II) Non-singular plane cubics:

$$C : \quad F(x, y, z) = 0$$

where F is a homogeneous cubic polynomial and the curve C is non-singular. Here C is a curve in the projective plane $\mathbb{P}^2$.

(III) Transverse intersection of quadric surfaces in $\mathbb{P}^3$. Let A be a 4×4 matrix with entries in K. The equation

$$\mathbf{x}^tA\mathbf{x} = 0, \qquad \mathbf{x} = (x_0 : x_1 : x_2 : x_3)$$

defines a quadric surface in $\mathbb{P}^3$ (degenerate if $\det(A) = 0$). Let B be another 4×4 matrix and consider their intersection

$$C \ : \quad \mathbf{x}^tA\mathbf{x} = 0, \quad \mathbf{x}^tB\mathbf{x} = 0.$$

The intersection is transverse if homogeneous quartic polynomial $\det(\lambda A + \mu B)$ does not have repeated factors. In this case C is a curve of genus 1.

(I), (II), (III) by no means exhaust the possible models for curves of genus 1, but these are the most important families that you should be aware of. We said that if curve C of genus 1 is defined over a field K, and has a K-rational point P_0, then there is a birational map $\phi : C \to E$ to a Weierstrass model E defined over K where $\phi(P_0) = O$. The existence of the map ϕ follows from the Riemann-Roch Theorem. Moreover, there are explicit recipes for transforming the above genus 1 models to Weierstrass equations (see [2, Chapter 8]). It is also possible to ask MAGMA to do this.

Example 2.1. Let C be the cubic curve (over $\mathbb{Q}$) given by

$$C \ : \quad 4u^3 - 2uvw - 18uw^2 - v^2w - 31w^3 = 0.$$

We note that C has the point $P_0 = (0 : 1 : 0)$. Let us see how we can obtain a Weierstrass model E and a map ϕ using MAGMA. Before we can specify the curve C we have to specify where it lives. We enter in MAGMA:

```
> PP<u,v,w>:=ProjectiveSpace(Rationals(),2);
```

This tells MAGMA that we are working in projective space PP over the rationals; the 2 is the dimension of PP, so PP is in fact the projective plane. The u, v, w are going to be our variables which we use to specify curves in PP. Let us now specify C:

```
> C:=Curve(PP,4*u^3 - 2*u*v*w - 18*u*w^2 - v^2*w - 31*w^3);
```

We want to specify the point $P_0 = (0 : 1 : 0)$ on C.

```
> P0:=C![0,1,0];
```

This tells MAGMA to think of the triple of numbers $[0, 1, 0]$ as the point $P0$ on C. Now let us construct E and ϕ in one go:

```
> E, phi:=EllipticCurve(C,P0);
```

Here [1] we are expecting MAGMA to return both the elliptic curve E and the map ϕ. Let us ask MAGMA for E and ϕ:

```
> E, phi;
Elliptic Curve defined by y^2 - 1/2*x*y = x^3 - 9/32*x - 31/256 over Rational
Field
Mapping from: CrvPln: C to CrvEll: E
with equations :
1/4*u
-1/16*v
w
and inverse
1/4*$.1
-$.2
1/16*$.3
```

This tells us that

$$E : y^2 - \frac{1}{2}xy = x^3 - \frac{9}{32}x - \frac{31}{256}, \qquad \phi(u : v : w) = (u/4w, -v/16w).$$

We can ask MAGMA for a nicer model for the curve E:

```
> SimplifiedModel(E);
Elliptic Curve defined by y^2 + x*y + y = x^3 - 5*x - 8 over Rational Field
```

[1]Note the command `EllipticCurve` is the same command as the one used in in Example 1.1 but that the input is different. Instead of giving the Weierstrass coefficients we are giving a curve of genus 1 and a rational point.

3. Everywhere Local Solubility

Let C be a curve of genus 1 defined over $\mathbb{Q}$. We want to know if $C(\mathbb{Q}) \neq \emptyset$. We do not have an algorithm that is guaranteed to determine if $C(\mathbb{Q})$ is non-empty ([2]). The easiest thing to do is to search for rational points on C. If we find one then we have answered our question.

Suppose that a search does not reveal any rational points on C. The next obvious thing to do is to look for some prime, such that C does not have points modulo that prime.

Example 3.1. Let $D/\mathbb{Q}$ be the curve

$$D \ : \quad x^3 + 2y^3 + 7z^3 = 0.$$

A short search for rational points does not reveal any. It is easy however to show that there aren't any points modulo 7, and hence there are no rational points.

Example 3.2. Let $D/\mathbb{Q}$ be the curve

$$D \ : y^2 = 8x^4 - 1.$$

It can be shown that D has points modulo any prime p, including of course 2. However, D has no solutions modulo 8.

Instead of asking if D has solutions modulo every power of the prime p, it is more convenient to ask if $D(\mathbb{Q}_p) \neq \emptyset$. These two questions are equivalent, but is easier to deal with $\mathbb{Q}_p$ because it is a field, whereas $\mathbb{Z}/p^r\mathbb{Z}$ is a ring with zero divisors. Let us look at another trivial example.

Example 3.3. Let $D/\mathbb{Q}$ be the curve

$$D \ : \quad -y^2 = x^4 + x + 1.$$

The polynomial on the right-hand side has no real roots. Thus $x^4 + x + 1 > 0$ for all x. Hence, $D(\mathbb{R}) = \emptyset$, and so there aren't any rational points because there are no real points.

The upshot of these meditations is the following: a necessary condition for $C(\mathbb{Q}) \neq \emptyset$ is that $C(\mathbb{Q}_p) \neq \emptyset$ for all primes p (including $p = \infty$, where $\mathbb{Q}_\infty = \mathbb{R}$).

More generally, let C be a curve of genus 1 over a number field K. We know that $K \subset K_\upsilon$ for any prime υ on K (including the infinite primes ([3])). Hence $C(K) \subset C(K_\upsilon)$ for any prime υ on K. If we can show that $C(K_\upsilon) = \emptyset$ for some υ, then we know that $C(K) = \emptyset$.

Definition. *We shall say that C has points everywhere locally (or C is everywhere locally soluble) if $C(K_\upsilon) \neq \emptyset$ for all υ. We say that C has global points if $C(K) \neq \emptyset$.*

Everywhere local solubility is a necessary condition for the existence of global points. Although we do not have an algorithm for deciding if $C(K) \neq \emptyset$, there is an algorithm for testing everywhere local solubility. In fact, all we have to check are the real infinite primes and the primes of 'bad reduction' for C, ask we explain just now.

Let υ be a finite (or archimedean) prime of K and let π be a uniformizer for υ. Suppose that C is given by an integral model (that means that there are no powers

[2]This intimately related to the fact that we do not have an algorithm for determining a Mordell-Weil basis for $E(\mathbb{Q})$ for Elliptic curve $E/\mathbb{Q}$.

[3]You might be used to calling infinite primes archimedean, and finite primes non-archimedean.

of π in the denominators of the coefficients of the equation defining C). Then we can reduce the equations defining C modulo π to obtain a curve $\tilde{C}$ over the finite field k_v. We say that v is a prime of good reduction for C if $\tilde{C}$ is non-singular [4]. A prime of **bad reduction** for C is a finite prime such that $\tilde{C}$ is singular.

Theorem 3. *If C is a curve of genus 1 and v is a prime of good reduction for C then $C(K_v) \neq \emptyset$.*

The proof of this result combines two very different techniques:

- A deep result due to F. K. Schmidt, which shows that $\tilde{C}(k_v) \neq \emptyset$.
- Hensel's Lemma, which treats the point on $\tilde{C}(k_v)$ as a first approximation to a v-adic point and gives better and better approximations that do converge to a point in $C(K_v)$.

It turns out that there are only finitely many primes of bad reduction for a given smooth curve C. For example, if $y^2 = f(x)$ where $f(x) \in \mathcal{O}_K[x]$ (i.e. a polynomial with integral coefficients) and $f(x)$ is separable (i.e. no repeated roots) then the primes of bad reduction all divide 2Δ, where Δ is the discriminant of f.

Moreover, Hensel's Lemma gives an algorithm for deciding the existence of local points even at bad primes.

Example 3.4. Let us look at the curve $y^2 = 2(x^4 - 17)$ using MAGMA.

```
> C:=HyperellipticCurve(2*(x^4-17));
> RationalPoints(C : Bound:=100);
{@ @}
```

We asked MAGMA to search for rational points on C with naive height at most 100. MAGMA didn't find any such points. Let us check everywhere local solubility.

```
> BadPrimes(C);
[ 2, 17 ]
> IsLocallySolvable(C,2);
true (-61866443383379 + O(2^47) : O(2^50) : 1 + O(2^50))
> IsLocallySolvable(C,7);
true (-3 + O(7) : -3 + O(7) : 1 + O(7^50))
```

The points given by MAGMA here are approximations which by Hensel's Lemma are known to lift to p-adic points on C. Of course, we mustn't forget about real solubility, but it is clear that $C(\mathbb{R}) \neq \emptyset$. We see that $C(\mathbb{Q}_p) \neq \emptyset$ for all primes p including ∞. It turns out that C does not have any rational points.

Example 3.5. Let us look at the curve

$$C \ : \quad x^2 + y^2 = z^2, \quad x^2 - y^2 = 17w^2.$$

We know that C is a curve of genus 1 (transverse intersection of two quadrics in $\mathbb{P}^3$).

[4] By demanding that $\tilde{C}$ be non-singular, we mean that $\tilde{C}$ has no singular points even over the algebraic closure of k_v

```
> PP<x,y,z,w>:=ProjectiveSpace(Rationals(),3);
> C:=Curve(PP,[x^2+y^2-z^2,x^2-y^2-17*w^2]);
> C;
Curve over Rational Field defined by
x^2 + y^2 - z^2,
x^2 - y^2 - 17*w^2
> RationalPoints(C : Bound:=100);
{@ @}
```

Now, for this model (intersection of two quadrics) there is no MAGMA command for the bad primes. However, you can check by hand that if $p \neq 2$, 17 then $\tilde{C}/\mathbb{F}_p$ is non-singular. Hence we know by Theorem 3 that $C(\mathbb{Q}_p) \neq \emptyset$ for $p \neq 2$, 17, ∞. For $p = \infty$ it is obvious that $C(\mathbb{R}) \neq \emptyset$.

```
> IsLocallySolvable(C,2);
true (68224686020887 + O(2^47) : O(2^47) : 68224686020887 + O(2^47) : 1 +
O(2^50))
> IsLocallySolvable(C,17);
true (741773957347780073472790517338923546888465111087237434262959 7 + O(17^50) :-741773957
O(17^50) : O(17^50))
```

Hence C is everywhere locally soluble.

4. Descent Arguments

In the previous section we saw two examples of curves that have points everywhere locally but there are no obvious global points. How can we prove that there aren't global points? The standard method is descent. Although there is perfectly respectable theory of descent (see for example Silverman's book [3], chapters 8 and 10), I believe that this best approached first through examples. Descent is really factorisation arguments applied to equations. At the heart of it is the following trivial observation based on the uniqueness of factorisation: if X, Y, Z are non-zero integers with $\gcd(X, Y) = 1$, n is a positive integer, and $XY = Z^2$ then $X = \pm Z_1^n$ and $Y = \pm Z_2^n$ for some integers Z_1, Z_2 satisfying $Z = Z_1 Z_2$. The observation needs to be adapted in obvious ways to different situations. Let us look now at a curve

$$C \ : \quad y^2 = f(x)g(x)$$

where $f(x) \in \mathbb{Z}[x]$, $g(x) \in \mathbb{Z}[x]$, the polynomials f, g are coprime and squarefree. Moreover, for simplicity suppose that $f(x)$ and $g(x)$ both have even degrees. Let us assume that C is everywhere locally soluble but we do not know if it has rational points. Write

$$x = \frac{X}{Z}, \qquad y = \frac{Y}{Z^2}$$

where X, Z are coprime integers. Then, clearing denominators we get

$$C \ : \quad Y^2 = F(X, Z)G(X, Z)$$

with F and G homogeneous binary forms.

Lemma 4.1. *Suppose a divides both $F(X, Z)$ and $G(X, Z)$ where X, Z are coprime integers. Then a divides the resultant $R = \mathrm{Res}(f, g)$.*

Proof. By the theory of resultants

$$u(x)f(x) + v(x)g(x) = R,$$

for some polynomials u and $v \in \mathbb{Z}[x]$. Clearing denominators we get

$$U(X,Z)F(X,Z) + V(X,Z)G(X,Z) = RZ^n$$

for some binary forms U, V and positive integer n. Thus a divides RZ^n.

We can do the same with the reverse polynomials of f and g which happen to have the same resultant. Hence a divides RX^m for some positive m. Since X and Z are coprime, a divides R. □

We see from the Lemma that if (X,Y,Z) is an integral solution to $Y^2 = F(X,Z)G(X,Z)$ then $F(X,Z) = aY_1^2$ and $G(X,Z) = aY_2^2$ for some squarefree integer a dividing R, where $Y = aY_1Y_2$.

Let D_a be the curve

$$D_a \ : \quad F(X,Z) = aY_1^2, \quad G(X,Z) = aY_2^2,$$

and $\phi_a : D_a \to C$ be the map

$$\phi_a(X : Y_1 : Y_2 : Z) = (X : aY_1Y_2 : Z).$$

The following lemma is clear from the discussion so far.

Lemma 4.2.

$$C(\mathbb{Q}) = \bigcup_{a|R} \phi_a(D_a(\mathbb{Q})).$$

We started out wanting to know to answer the question: does C have rational points? The above transforms this question into: do any of the D_a have rational points?

The curves D_a are called coverings of C. Of course if $D_a(\mathbb{Q}_p) = \emptyset$ for some prime p then $D_a(\mathbb{Q}) = \emptyset$ and we may exclude this particular D_a. We let

$$A = \{a \ : \ a \text{ divides } R \text{ and } D_a(\mathbb{Q}_p) \neq \emptyset \text{ for all primes } p\}.$$

We only want to keep D_a for $a \in A$. In other words, we want the everywhere locally soluble coverings. We can improve our lemma above to the following theorem.

Theorem 4.

$$C(\mathbb{Q}) = \bigcup_{a \in A} \phi_a(D_a(\mathbb{Q})).$$

Example 4.1. Let us take another look at the curve treated in Example 3.5,

$$C \ : \quad x^2 + y^2 = z^2, \quad x^2 - y^2 = 17w^2.$$

Recall that C is everywhere locally soluble but that we have been unable to find rational points on C.

Let us show that C has no rational points, despite having points everywhere locally. Suppose $(x : y : z : w)$ is a rational point on C. The first equation $x^2 + y^2 = z^2$ is a circle (projectively) and you probably know the parametrisation

$$(x : y : z) = (m^2 - n^2 : 2mn : m^2 + n^2)$$

for some m, $n \in \mathbb{Q}$. By scaling x, y, z, w we obtain $x = m^2 - n^2$, $y = 2mn$, $z = m^2 + n^2$. Substituting in the second equation $x^2 - y^2 = 17w^2$ we get

$$C' \ : \quad (m^2 + 2mn - n^2)(m^2 - 2mn - n^2) = 17w^2.$$

All we have done so far is constructed another model C', birational to C, which is more convenient to work with. Since C and C' are birational over $\mathbb{Q}$, we have $C'(\mathbb{Q}_p) \neq \emptyset$ for all primes p. Moreover C' has rational points if and only if C has rational points. Next, we do a descent. We may suppose that m, n are pairwise coprime integers. It is easy to see then that the two factors $m^2 + 2mn - n^2$, $m^2 - 2mn - n^2$ cannot simultaneously be divisible by an odd prime. Hence

$$D_a \ : \quad m^2 + 2mn - n^2 = aw_1^2, \quad m^2 + 2mn - n^2 = 17aw_2^2$$

where a is some divisor of 34 (i.e. some element of $\{\pm 1, \pm 2, \pm 17, \pm 34\}$). We can also reverse the factorisation argument: for any a we have a map

$$\phi_a \ : \quad D_a \to C', \qquad \phi_a(m : n : w_1 : w_2) = (m, n, aw_1w_2).$$

It is clear from our descent (i.e. factorisation) argument that

$$C'(\mathbb{Q}) = \bigcup_{a|34} \phi_a(D_a(\mathbb{Q})).$$

We can check that $D_a(\mathbb{Q}_{17}) = \emptyset$ for possible values of a. Hence $D_a(\mathbb{Q}) = \emptyset$.

4.1. **The Hasse Principle.** We have met curves of genus 1, but skipped over curves of genus 0. A curve of genus 0 is birational to a conic in $\mathbb{P}^2$. Curves of genus 0 satisfy the following nice property: if C is a curve of genus 0 over a number field K, and C has points everywhere locally then C has global points. This property is known as the **Hasse Principle**. It holds for curves of genus 0, but often fails for curves of genus 1, as we saw in Example 4.1. Such an example is called a **counterexample to the Hasse principle**.

5. Exercises

A famous theorem of Faltings says that if C is a curve of genus $g \geq 2$ over a number field K then $C(K)$ is finite.

A typical curve of genus 2 is of the form $y^2 = h(x)$ where h is squarefree of degree 5 or 6. It is sometimes possible to combine the descent strategy of the previous section, with what we have learned about curves of genus 1 to write down all the rational points on curves of genus 2.

Exercise 5.1. Let C be the genus 2 curve

$$C \ : \quad y^2 = 4x^6 + 4x^4 + 1.$$

Construct two (non-constant) maps $\phi_i : C \to E_i$ where E_i are Weierstrass elliptic curves. Calculate the Mordell-Weil groups of the E_i (use MAGMA or any other program you like). Find $C(\mathbb{Q})$ (don't forget about the points at infinity).

Exercise 5.2. Consider the genus 2 curve

$$C \ : \quad y^2 = (x^2 + 3x + 1)(x^4 + 1).$$

(i) Make a list of the obvious rational points that you can see on C (do forget about the points at infinity).
(ii) Carry out the descent strategy explained in the previous section. Hence show that $C(\mathbb{Q}) = \phi(D(\mathbb{Q}))$ where

$$D \ : \quad y_1^2 = x^2 + 3x + 1, \quad y_2^2 = x^4 + 1.$$

(iii) Let F be the genus 1 curve $y_2^2 = x^4 + 1$. Transform this to a Weierstrass equation and calculate its Mordell-Weil group (use MAGMA or any other package if you like).

(iv) Use your answer to part (iii) to calculate $D(\mathbb{Q})$ and hence $C(\mathbb{Q})$.

Exercise 5.3. We show that $C(\mathbb{Q}) = \emptyset$ for C in Example 3.4. This exercise is adapted from Cassels [2, page 88], and requires some algebraic number theory. In particular, you will need to know that $\mathbb{Q}(\sqrt{17})$ has class number 1, that its ring of integers is $\mathcal{O} = \mathbb{Z}[\theta]$ where $\theta = (1+\sqrt{17})/2$ and that $\eta = 4+\sqrt{17}$ is a fundamental unit.

Observe that it is enough to show that the equation $a^4 - 17c^4 = 2b^2$ has no solutions with a, b, c integers, $\gcd(a, c) = 1$. Suppose there is such a solution.

(a) Show that a, c are both odd and that the two algebraic integers

$$\frac{a^2 + c^2\sqrt{17}}{2}, \quad \frac{a^2 - c^2\sqrt{17}}{2}$$

are coprime.

(b) Hence

$$\frac{a^2 + c^2\sqrt{17}}{2} = \frac{\pm 5 \pm \sqrt{17}}{2}\eta^r \mu^2$$

for some $\mu \in \mathcal{O}$.

(c) Show that r must be even (note $\mathrm{Norm}(\eta) = -1$). Thus we can absorb η^r in μ^2 to get

$$\frac{a^2 + c^2\sqrt{17}}{2} = \frac{\pm 5 \pm \sqrt{17}}{2}\mu^2.$$

(d) Put $\mu = (u + v\sqrt{17})/2$ where u, v are in $\mathbb{Z}$. Equating the coefficients of 1 and $\sqrt{17}$ on both sides obtain coverings and show that these are not everywhere locally soluble. Thus $C(\mathbb{Q}) = \emptyset$.

References

[1] W. Bosma, J. Cannon and C. Playoust, *The Magma Algebra System I: The User Language*, J. Symb. Comp. **24** (1997), 235–265. (See also `http://www.maths.usyd.edu.au:8000/u/magma/`)

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

[3] J. H. Silverman, *Arithmetic of Elliptic Curves*, Springer-Verlag, 1992.

Samir Siksek, Mathematics Institute, University of Warwick, Coventry, CV4 7AL, United Kingdom

E-mail address: `samirsiksek@yahoo.com`