Some ternary Diophantine equations of signature $(n, n, 2)$

Nils Bruin[1]

Simon Fraser University. Email: bruin@member.ams.org

Summary. In this article, we will determine the primitive integral solutions x, y, z to equations of the form

$$x^n + y^n = Dz^2$$

with $n = 4, 5, 6, 7, 9, 11, 13, 17$ and $D \in \{2, 3, 5, 6, 10, 11, 13, 17\}$.

These equations form the small exponent cases of the equations considered by Bennett and Skinner in [1], where their modular techniques do not apply.

The computations necessary form a nice showcase of the arithmetic geometric functionality in the Magma computer algebra system. We will show how to construct curves, how to test curves for local solubility, how to analyse elliptic curves over number fields and how to use Chabauty-techniques to determine the rational points on a curve.

1 Introduction

The following result is stated in the paper [1] by Bennett and Skinner.

Theorem 1. *If $n \geq 4$ is an integer and*

$$D \in \{2, 3, 5, 6, 10, 11, 13, 17\}$$

then the equation

$$x^n + y^n = Dz^2$$

has no solutions in nonzero coprime integers (x, y, z) with, say, $x > y$, unless $(n, D) = (4, 17)$ or $(n, D, x, y, z) \in \{(5, 2, 3, -1, \pm 11), (5, 11, 3, 2, \pm 5)\}$.

In that paper the authors use techniques based on Galois representations on torsion subgroups of elliptic curves and modular forms to prove a large part of this theorem, but these methods do not apply to all combinations of

[1] The research described in this paper is partly funded by NSERC and the University of Sydney.

n, D that occur in the statement and for each $n \leq 17$, there are some values of D for which they refer to this paper rather than give a proof. Indeed, here we we will prove the following result.

Theorem 2. *If $n \in \{5, 6, \ldots, 17\}$ and $D \in \{2, 3, 5, 6, 10, 11, 13, 17\}$ then the equation*

$$x^n + y^n = Dz^2$$

has no solutions in coprime nonzero integers except those arising from the identities $1^n + 1^n = 2 \cdot 1^2$, $3^5 - 1^5 = 2 \cdot 11^2$ and $3^5 + 2^5 = 11 \cdot 5^2$.

We will also prove

Proposition 1. *The equation $x^4+y^4 = Dz^2$ has no integral solutions for $D \in \{3, 5, 6, 10, 11, 13\}$. For $D = 2$, the only integral solutions with $\gcd(x, y, z) = 1$ are $(x, y, z) = (\pm 1, \pm 1, \pm 1)$. For $D = 17$, it has infinitely many integral solutions with distinct values of x/y.*

We will use the proofs to introduce the reader to some of the very powerful tools that Magma offers for solving arithmetic geometric questions. The article is laid out in the following way.

As an introduction we give an easy proof to Proposition 1. It shows the basic mechanisms that are available in Magma to define arithmetic geometric objects and answer questions about them. We try to point out that many questions can be formulated and answered using Magma in a language that is very close to the one that mathematicians are used to.

Next, we review some mathematical concepts and constructions that will prove indispensible in the rest of the paper. We recall a theorem from [5] that translates questions like the one in Theorem 2 to questions about rational points on some algebraic curves.

In Section 4, we apply those results to $x^5 + y^5 = Dz^2$ and, using Magma, obtain some curves that parametrise the primitive solutions to the equation under consideration. We then construct elliptic subcovers of those curves such that an application to them of the methods from [5] yields the rational points on the original curves. We defer the actual application to Section 7.

We trust that after this demonstration of the problem solving capability of Magma, the reader will be interested in knowing some of the algorithms employed. In Section 5 we give a full account of the algorithms the author has implemented in Magma to test schemes for local solvability. A highlight is an algorithm that decides local solvability of hyperelliptic curves in time that is essentially independent of the size of the residue class field in the odd residue characteristic case.

In Section 6, we explain how 2-Selmer groups and 2-isogeny Selmer groups of elliptic curves over number fields can be computed, how they can be used to bound the free ranks of Mordell-Weil groups and how they can be used to find generators for Mordell-Weil groups. We also explain how one can do this in Magma using the implementation of the author, based on [3].

In Section 7, we explain how the techniques first introduced in [2] can be applied to use elliptic curves over number fields to find the rational points on curves. We outline how one can use the implementation by the author to prove the result in Theorem 2 for $n = 5$.

In the last section, we give an outline of successfull strategies to solve the remaining cases from Theorem 2. For full details and a transcript of the Magma session that obtains all computational results in this paper, we refer the reader to the electronic resource [6].

2 Proof of Proposition 1

To get a taste for things to come, we first prove Proposition 1. It is very straightforward. First note that any solution to $x^4 + y^4 = Dz^2$ corresponds to a rational point $(u, v) = (x/y, Dz/y)$ on the curve

$$D(u^4 + 1) = v^2.$$

We can simply ask Magma to compute for each desired value of D, whether this curve has any points over, say, $\mathbb{Q}_2$ (see Section 5.4).

```
> _<x>:=PolynomialRing(Rationals());
> Dset:={2,3,5,6,10,11,13,17};
> {D:D in Dset| IsLocallySolvable(HyperellipticCurve(D*(x^4+1)),2)};
{ 2, 17 }
```

So just by testing local solvability at 2, we have already proved the lemma for all values of D except 2 and 17. Let's first consider $D = 2$. Clearly, the curve $2u^4 + 2 = v^2$ has a rational point $(u, v) = (1, 2)$, so it is isomorphic to an elliptic curve E. The rational points of an elliptic curve form a finitely generated group. Magma can compute an upper bound on the free rank of that group (see Section 6) and as it turns out, it is 0.

```
> C2:=HyperellipticCurve(2*(x^4+1));
> p0:=C2![1,2];
> E,C2toE:=EllipticCurve(C2,p0);
> RankBound(E);
0
> #TorsionSubgroup(E);
4
```

We find an upper bound of 0 on the free rank, so $E(\mathbb{Q})$ consists entirely of torsion points, of which there are 4. Indeed, there are 4 obvious points:

$$(u, v) = (1, 2), (-1, 2), (1, -2), (-1, -2).$$

and these all correspond to solutions with $x = \pm y$.

For $D = 17$ we proceed similarly. We find the point $(u, v) = (2, 17)$ on the curve $17u^4 + 17 = v^2$. This time we find an upper bound of 2 on the free rank.

```
> C17:=HyperellipticCurve(17*(x^4+1));
> p0:=C17![2,17];
> E,C17toE:=EllipticCurve(C17,p0);
> RankBound(E);
2
```

In fact, Magma can find two independent points on E (note that the command `MordellWeilGroup` in principle could return a group of smaller rank, so one should always check that the rank of the returned group corresponds to the expected rank).

```
> G,GtoE:=MordellWeilGroup(E);
> G;
Abelian Group isomorphic to Z/2 + Z/2 + Z + Z
Defined on 4 generators
Relations:
    2*G.1 = 0
    2*G.2 = 0
> [Inverse(C17toE)(GtoE(g)):g in OrderedGenerators(G)];
[ (-1 : 17 : 2), (-2 : -17 : 1), (13 : 697 : 2), (314 : 3097553 : 863) ]
```

The last solution corresponds to the primitive solution:

$$(2 \cdot 157)^4 + 863^4 = 17 \cdot (182209)^2$$

and, using the group law on E, arbitrarily many can be constructed.

3 Construction of parametrising curves

In this section, we recall a result from [14] in an explicit form, occurring in [2], which relates integer solutions (x, y, z) of equations like $x^n + y^n = Dz^m$ with $\gcd(x, y, z) = 1$ to rational points on some algebraic curves.

First we need some notation.

Let $f(x, y) \in \mathbb{Z}[x, y]$ be a square-free homogeneous form of degree n and assume for simplicity that $f(x, 1)$ is monic of degree n, i.e, $f(x, y) = x^n + y(\cdots)$. We construct the algebra $A = Q[\theta] = Q[x]/f(x, 1)$. This allow us to express f as a *norm form*

$$f(x, y) = N_{A[x,y]/\mathbb{Q}[x,y]}(x - \theta y).$$

Let S be a finite set of rational primes and let K be a number field. For a prime $\mathfrak{p}$ of K we write $\mathfrak{p} \nmid S$ is $\mathfrak{p}$ does not extend any prime in S to K. Following [21], we define

$$K(p, S) := \{a \in K^* : v_{\mathfrak{p}}(a) \equiv 0 \pmod{p} \text{ for all primes } \mathfrak{p} \nmid S\}/K^{*p}.$$

Following Magma's terminology, we refer to this set as the (p, S)-*Selmer group* of K. It is a finite, effectively computable group. An algorithm for computing

it is described in [19] and the implementation and optizations in MAGMA are due to Fieker [15].

Since f is square-free, the algebra A is isomorphic to a direct product of number fields $K_1 \times \cdots \times K_r$. We generalise the notation above to

$$A(p, S) := K_1(p, S) \times \cdots \times K_r(p, S) \subset A^*/A^{*p}.$$

Furthermore, we will identify elements of $A(p, S)$ with some set of representatives in A^*.

Since $\{1, \theta, \ldots, \theta^{n-1}\}$ forms a $\mathbb{Q}[Z_0, \ldots, Z_{n-1}]$-basis of the vector space $A[Z_0, \ldots, Z_{n-1}]$, for any $\delta \in A^*$ there are unique homogeneous forms $Q_i = Q_{\delta,i} \in \mathbb{Q}[Z_0, \ldots, Z_{n-1}]$ of degree m such that

$$Q_0 + Q_1\theta + \cdots + Q_{n-1}\theta^{n-1} = \delta(Z_0 + Z_1\theta + \cdots + Z_{n-1}\theta^{n-1})^m.$$

We define the projective curve

$$C_\delta := \{Q_2 = Q_3 = \cdots = Q_{n-1} = 0\} \subset \mathbb{P}^{n-1}$$

and the map $\phi_\delta : C_\delta \to \mathbb{P}^1$ defined by

$$\phi_\delta : (Z_0 : \cdots : Z_{d-1}) \mapsto -\frac{Q_0(Z_0, \ldots, Z_{n-1})}{Q_1(Z_0, \ldots, Z_{n-1})}.$$

From [2, Theorem 3.1.1], it follows that C_δ is absolutely irreducible of genus $1 + m^{n-2}(\frac{1}{2}n(m-1) - m)$ and that ϕ_δ is a Galois cover with Galois-group $(\mathbb{Z}/m\mathbb{Z})^{n-1}$, ramified exactly at $\{(x : y) \in \mathbb{P}^1(\overline{\mathbb{Q}}) : f(x, y) = 0\}$.

For given nonzero integer D and $m \geq 1$, we consider the equation

$$f(x, y) = Dz^m.$$

Let S be a finite set of primes containing the prime divisors of $D\mathrm{Disc}(f)$.

$$\Delta := \{\delta \in A(m, S) : N_{A/\mathbb{Q}}(\delta)/D \in \mathbb{Q}^{*m}\}.$$

A consequence of [2, Lemma 3.1.2] is

Theorem 3. *Let $f, D, m, \theta, A, \Delta$ be defined as above. Then*

$$\left\{(x : y) : x, y, z \in \mathbb{Z}, f(x, y) = Dz^m, \gcd(x, y, z) = 1\right\} \subset \bigcup_{\delta \in \Delta} \phi_\delta(C_\delta(\mathbb{Q}))\}$$

One can easily recover (x, y, z) from $(x : y)$ in the following way. Let $(x_0 : y_0) \in \mathbb{P}^1(\mathbb{Q})$. If (x, y, z) is a solution with $(x : y) = (x_0 : y_0)$, then there is a $\lambda \in \mathbb{Q}^*$ such that

$$\begin{aligned} x &= \lambda x_0, \\ y &= \lambda y_0, \\ z &= \sqrt[m]{\frac{\lambda^n f(x_0, y_0)}{D}}. \end{aligned}$$

Given x_0, y_0, it is straightforward to determine for which values of λ the above system has solutions with $\gcd(x, y, z) = 1$ and what those solutions are.

The strategy for proving Theorem 2 is to determine the relevant curve C_δ for each of the combinations (n, D) and to find the rational points on C_δ. In some cases we get away with only constructing a subcover of $C_\delta/\mathbb{P}^1$.

In the particular, when m divides n, then the weighted projective equivalence classes of solutions to $f(x, y) = Dz^m$ are in bijection with the rational points of the curve given by the weighted projective model $C' : f(x, y) = Dz^m$, where (x, y, z) have weights $(1, 1, n/m)$. In the special case that $m = 2$, we see that C' is a double cover of a projective line. The curves C_δ are twists of the unramified cover of C' obtained by embedding C' in its jacobian $\mathrm{Jac}(C')$ and taking the pullback along the multiplication-by-2 map on $\mathrm{Jac}(C')$. These properties are explained and exploited in [8] and in a trivial way in Section 8.

In the particular case that $m = 2$ and $n = 4$, we recover the multiplication-by-2 covers of curves of genus 1 that play a role in 2-descents and 4-descents. If f has a rational root, then C' is isomorphic to its jacobian and the C_δ are the homogeneous spaces that play a role in 2-descents as described in Section 6.

If f does not have a rational root, then C' can still be expressed as a $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ cover of its jacobian. The C_δ are then homogeneous spaces associated to a 4-descent on the jacobian. See [18] and [25].

4 The equation $x^5 + y^5 = Dz^2$

We begin putting the construction from Section 3 into Magma. In our case $f = x^5 + y^5$. We model this by defining a univariate polynomial in Magma. This allows us to construct the algebra straight away.

```
> _<x>:=PolynomialRing(Rationals());
> f:=x^5+1;
> A<theta>:=quo<Parent(x)|f>;
```

Next we construct the rings $A[Z_0, \ldots, Z_4]$, $\mathbb{Q}[Z_0, \ldots, Z_4]$ and the corresponding projective space. Note that, while mathematically

$$\mathbb{Q}[\theta][Z_0, \ldots, Z_4] \simeq \mathbb{Q}[Z_0, \ldots, Z_4][\theta]$$

in a canonical way, this is not the case in a computer algebra system. We first construct the left hand side (`PA`) and then obtain the right hand side (`AP`) using `SwapExtension`. We also get the appropriate isomorphism `swap`. We then extract $\mathbb{Q}[Z_0, \ldots, Z_4]$ as the base ring of `AP`.

```
> PA<Z0A,Z1A,Z2A,Z3A,Z4A>:=PolynomialRing(A,5);
> AP<thetaP>,swap:=SwapExtension(PA);
> _<Z0,Z1,Z2,Z3,Z4>:=BaseRing(AP);
> P4:=Proj(BaseRing(AP));
> P1:=ProjectiveSpace(Rationals(),1);
```

Given $\delta \in A$, it is now straightforward to construct C_δ and ϕ_δ. We present a Magma routine that takes δ as input and returns both C_δ and ϕ_δ. Note that `Coefficients` on an element of `AP` returns a sequence of coefficients with respect to the power basis $[1, \theta, \ldots, \theta^4]$, i.e., the Q_i for us.

```
> function Cdelta(delta)
function>   g:=delta*(&+[PA.i*theta^(i-1): i in [1..5]])^2;
function>   Q:=Coefficients(swap(g));
function>   Crv:=Scheme(P4,[Q[3],Q[4],Q[5]]);
function>   phi:=map<Crv->P1|[Q[1],-Q[2]]>;
function>   return Crv,phi;
function> end function;
```

Given D, we can compute the set Δ as well. For that, we need to represent $\mathbb{Q}$ as a number field `Q` and A as an algebra over `Q`. We also compute the decomposition of $A = \mathbb{Q} \times K$, where $K = \mathbb{Q}(\zeta)$, the field generated by a primitive 5th root of unity. By giving an explicit representation to `AbsoluteAlgebra`, we make sure the system uses that representation.

```
> Q:=NumberField(x-1:DoLinearExtension);
> OQ:=IntegerRing(Q);
> Qx<xQ>:=PolynomialRing(Q);
> AQ:=quo<Qx|Polynomial(Q,f)>;
> AQtoA:=hom<AQ->A|[theta]>;
> K<zeta>:=NumberField(x^4 - x^3 + x^2 - x + 1);
> OK:=IntegerRing(K);
> Aa,toAa:=AbsoluteAlgebra(AQ:Fields:={Q,K});
```

We can now compute Δ in the following way. We take S to be the set of primes that divide $D\mathrm{Disc}(f)$. We compute the subgroup of $A(2, S)$ that has square norm and we translate it over the class of D in $A(2, S)$.

```
> function DeltaForD(D)
function>   S:=Support(D*Discriminant(f)*OQ);
function>   slmA,slmAmap:=pSelmerGroup(AQ,2,S);
function>   slmQ,slmQmap:=pSelmerGroup(2,S);
function>   slmNorm:=map<slmA->slmQ|a:->slmQmap(Norm(a@@slmAmap))>;
function>   slmSquareNorm:=Kernel(hom<slmA->slmQ|
function>            [slmNorm(a):a in OrderedGenerators(slmA)]>);
function>   classD:=slmAmap(D);
function>   return {AQtoA( (d-classD)@@slmAmap):d in slmSquareNorm};
function> end function;
```

We gather all δs that are relevant together (remember we can always recover the corresponding D from $N_{A/\mathbb{Q}}(\delta)$) and throw out any for which C_δ is not locally solvable at 2, 5 or 11 (other primes turn out to make no further contributions).

```
> Dset:={2,3,5,6,10,11,13,17};
> BigDelta:=&join{DeltaForD(D):D in Dset};
> Delta:=BigDelta;
> Delta:={delta:delta in Delta| IsLocallySolvable(Cdelta(delta),2:
>                       AssumeIrreducible,AssumeNonsingular)};
> Delta:={delta:delta in Delta| IsLocallySolvable(Cdelta(delta),5:
>                       AssumeIrreducible,AssumeNonsingular)};
> Delta:={delta:delta in Delta| IsLocallySolvable(Cdelta(delta),11:
>                       AssumeIrreducible,AssumeNonsingular)};
```

This eliminates already 4/5th of the parametrising curves. Now we construct a subcover, derived from the ring homomorphism $m_1 : A \to \mathbb{Q}$ given by $\theta \mapsto -1$. From $x - \theta y = \delta c_0^2$, it follows that $f(x, y) = N_{A/\mathbb{Q}}(\delta)N_{A/\mathbb{Q}}(c_0)^2$. Hence,

$$x^4 - x^3y + x^2y^2 - xy^3 + y^4 = f(x, y)/m_1(x - \theta y) = N(\delta)/m_1(\delta)N(c_0)^2.$$

Putting $d = N(\delta)/m_1(\delta)$, it follows that C_δ covers

$$E_d : u^4 - u^3 + u^2 - u + 1 = dv^2.$$

We compute which curves occur.

```
> m1:=hom<A->Rationals()|-1>;
> {PowerFreePart(Norm(delta)/m1(delta),2):delta in Delta};
{ 1, 5, 55 }
```

Unfortunately, E_d has infinitely many rational points for $d = 1, 55$. For $d = 5$ we do get some useful information.

```
> E5:=HyperellipticCurve(5*(x^4-x^3+x^2-x+1));
> p0:=E5![-1,5];
> ell:=EllipticCurve(E5,p0);
> RankBound(ell);
0
> #TorsionSubgroup(ell);
2
```

We see that E_5 only has two rational points $(-1, \pm 5)$. It is straightforward to check that these correspond to the obvious solutions $(x, y, z) = (1, -1, 0), (-1, 1, 0)$ for $x^5 + y^5 = Dz^2$. If we take heed of these solutions, we can discard any δ for which C_δ covers E_5.

```
> Delta:={delta:delta in Delta|PowerFreePart(Norm(delta)/m1(delta),2) ne 5};
> #Delta;
16
```

For these remaining values, we use the same idea as above, but now we use the map $m_2 : A \to K$ given by $\theta \mapsto \zeta$. We define $d = N(\delta)/m_2(\delta)$ and we obtain the following subcover of $C_\delta/\mathbb{P}^1$.

$$E_d : u^4 + \zeta u^3 + \zeta^2 u^2 + \zeta^3 u + \zeta^4 = dv^2$$

where the cover $\phi_\delta : C_\delta \to \mathbb{P}^1$ induces the cover $u : E_d \to \mathbb{P}^1$. Since the value of d only matters up to squares, we take unique representatives by mapping through $K(2, S')$ for an appropriate S'.

```
> m2:=hom<A->K|zeta>;
> slmK,slmKmap:=pSelmerGroup(2,Support(2*3*5*11*13*17*OK));
> dset:={K|(slmKmap(Norm(delta)/m2(delta)))@@slmKmap:delta in Delta};
> dset;
{
    2*zeta^3 - 2*zeta^2 - 2,
    1,
    15*zeta^3 - 5*zeta^2 + 8*zeta - 17,
    -3*zeta^3 - 7*zeta^2 - 8*zeta - 9,
    -2*zeta^2 - 2
}
```

For our subsequent operations, it is beneficial to compute a Weierstrass model of E_d using the point $(u, v) = (-1, 0)$. We express the function u in the coordinates of that model. We obtain

$$E_d : Y^2 = X^3 - d(3\zeta^3 + \zeta - 1)X^2 - d^2(\zeta^2 + \zeta + 1)X$$

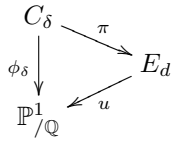
and

$$u = \frac{-X + d(\zeta^3 - 1)}{X - d(\zeta^3 + \zeta)}.$$

Using Magma, one can verify this using a few lines of code. Notice that the elliptic curve is represented as a *projective* curve.

```
> Kd<d>:=RationalFunctionField(K);
> KdX<X>:=PolynomialRing(Kd);
> FEd1:=(X^4+zeta*X^3+zeta^2*X^2+zeta^3*X+zeta^4)/d;
> Ed1:=HyperellipticCurve(FEd1);
> Ed2,toEd2:=EllipticCurve(Ed1,Ed1![-1,0]);
> umap:=map<Ed1->P1|[Ed1.1,Ed1.3]>;
> FEd:=X^3+(-3*zeta^3-zeta+1)*d*X^2+(-zeta^2-zeta-1)*d^2*X;
> Ed<xE,yE,zE>:=EllipticCurve(FEd);
> bl,toEd:=IsIsomorphic(Ed2,Ed);
> u:=Expand(Inverse(toEd2*toEd)*umap);
> u:Minimal;
(xE : yE : zE) -> ((-2*zeta^3 + 3*zeta^2 - 3*zeta + 2)/d^2*xE + (-zeta^3 - 2*zeta + 2)/d>
    (2*zeta^3 - 3*zeta^2 + 3*zeta - 2)/d^2*xE + (2*zeta^2 - zeta + 2)/d*zE)
```

We have the following diagram of covers.



Clearly,

$$\phi_\delta(C_\delta(\mathbb{Q})) \subset u(E_d(K)) \cap \mathbb{P}^1(\mathbb{Q}).$$

We can now complete the proof of Theorem 2 for $n = 5$ by computing the right hand side of the above inclusion. By techniques we will explain in Section 7, we find the following table.

d	$u(E_d(K)) \cap \mathbb{P}^1(\mathbb{Q})$
1	$\{-1, 0, \infty\}$
$-2\zeta^2 - 2$	$\{-1, 1\}$
$2\zeta^3 - 2\zeta^2 - 2$	$\{-3, -1, -1/3\}$
$-3\zeta^3 - 7\zeta^2 - 8\zeta - 9$	$\{-1, 3/2\}$
$15\zeta^3 - 5\zeta^2 + 8\zeta - 17$	$\{-1, 2/3\}$

It is straightforward to check that all of these values for x/y lead to solutions with $xyz = 0$ or solutions that are mentioned in Theorem 2.

5 Deciding local solvability

As we have seen in Sections 2 and 4, the first step in solving arithmetic geometric questions often involves deciding if, for a projective variety X over a number field K, the set $X(K_\mathfrak{p})$ is empty for some prime $\mathfrak{p}$. In this section, we outline several algorithms that have been implemented in Magma by the author to test local solvability. They include tools for determining the $K_\mathfrak{p}$-points of separated 0-dimensional schemes, $K_\mathfrak{p}$-solvability of complete intersections, $K_\mathfrak{p}$-solvability of smooth projective curves, given by a possibly singular planar model and $K_\mathfrak{p}$-solvability of hyperelliptic curves.

For the rest of this section, $\mathcal{O}$ will be a complete local ring of characteristic 0 with maximal ideal $\mathfrak{p}$ and finite residue field $\mathcal{O}/\mathfrak{p}$. We write π for a generator of $\mathfrak{p}$ and L for the field of fractions of $\mathcal{O}$. We use $\nu : L^* \to \mathbb{Z}$ to denote the normalised valuation, i.e., $\nu(\pi^e) = e$ and use the customary extension $\nu(0) = \infty$.

For any object f (vector, matrix, polynomial) defined over $\mathcal{O}$, we write $\overline{f}$ for the corresponding reduced object over $\mathcal{O}/\pi$. We also write $\nu(f)$ for the minimum of $\nu(c)$, where c runs through the coefficients of f.

5.1 Determining $X(L)$ for a reduced 0-dimensional projective scheme

Let $\mathbb{P}^n$ be n-dimensional projective space over K with variables $(X_0 : \ldots : X_n)$ and let X be a reduced 0-dimensional projective scheme, defined by

$$f_1 = \cdots = f_m = 0,$$

where $f_i \in K[X_0, \ldots, X_m]$. Without loss of generality, we can assume $f_i \in \mathcal{O}[X_0, \ldots, X_m]$.

Note that any point in $\mathbb{P}^n(L)$ has a representative $(x_0 : \cdots : x_n)$ such that for some $0 \leq N \leq n$, we have

$$(x_1, \ldots, x_{N-1}, x_N, x_{N+1}, \ldots, x_n) \in \mathcal{O} \times \cdots \times \mathcal{O} \times \{1\} \times \mathfrak{p} \times \cdots \times \mathfrak{p}$$

Hence, it is sufficient to solve the problem of finding $\mathcal{O}$-*integral* points on an *affine* separated 0-dimensional scheme Y, given by equations $f_i \in \mathcal{O}[\mathbf{y}] = \mathcal{O}[y_1, \ldots, y_n]$.

In principle, one could solve the problem in the same way as one does for exactly representable fields like $\mathbb{Q}$, $\mathbb{F}_q$ and number fields, by using resultants and univariate factorisation. In practice, however, the objects considered are not exactly represented and it is almost impossible to make such algorithms numerically stable. Therefore, we will present an algorithm here that simply builds solutions one π-adic digit at the time, until the solution is verifyably separated and Hensel liftable. We simply reduce the system of equations to $\mathcal{O}/\mathfrak{p}$, determine the solutions over that finite field and interpret what these solutions mean over $\mathcal{O}$.

The first step is to pick $g_i \in \mathcal{O}[\mathbf{y}]$ such that

$$(g_1, \ldots, g_m)\mathcal{O}[\mathbf{y}]$$

is as close as possible to

$$I = (f_1, \ldots, f_m)K[\mathbf{y}] \cap \mathcal{O}[\mathbf{y}].$$

Let

$$M_f = \left(\frac{\partial}{\partial y_j} f_i\right)_{i,j} \in \mathcal{O}^{m \times n}$$

Algorithm Saturate$(f_1, \ldots, f_m)$:

1. REPEAT
2. Let $T \in \mathrm{GL}_m(\mathcal{O})$ such that $\overline{T(M_f(0, \ldots, 0))}$ is in row echelon form.
3. $(f_1, \ldots, f_m)^t \leftarrow T(f_1, \ldots, f_m)^t$.
4. FOR $i \in \{1, \ldots, m\}$:
5. $\quad f_i \leftarrow f_i/\pi^{\nu(f_i)}$
6. UNTIL in step 5 no f_i was changed.
7. RETURN $(f_1, \ldots, f_m)$

This algorithm does not always find generators of I. However, if $(0, \ldots, 0)$ is sufficiently close to a non-singular point of Y, then for all $f \in I$, the minimal valuation of the coefficients of f is attained by the coefficient of a linear term. It is clear that in this situation, the algorithm will find g_i that generate I.

In practice, the coefficients of f_i are only given up to finite precision. Hence, in step 5, it might happen that a coefficient has no precision left. In that case, an error should be generated.

It is now straightforward to determine the integer points of Y up to some precision bound r:

Algorithm IntegerPoints$(r, f_1, \ldots, f_m)$:

1. $(f_1, \ldots, f_m) \leftarrow \text{Saturate}(f_1, \ldots, f_m)$.
2. Let $V \subset \mathcal{O}^n$ be a set of representatives of the solutions of $\overline{f_1} = \cdots = \overline{f_m} = 0$ in $\mathcal{O}/\mathfrak{p}$.
3. Let $V_0 \subset V$ represent the points over $\mathcal{O}/\mathfrak{p}$ with 0-dimensional tangent space.
4. $W \leftarrow \{\}$; $V_1 = V \setminus V_0$
5. FOR $v \in V_0$:
6. $\quad v \leftarrow$ Hensel lift of v to precision r using a suitable subset $\{f_{i_1}, \ldots, f_{i_n}\}$
7. $\quad$ IF for all i we have $\nu(f_i(v)) \geq r$ THEN
8. $\quad\quad$ Add v to W
9. $\quad$ ELSE
10. $\quad\quad$ Discard v
11. FOR $v \in V_1$:
12. $\quad g_i \leftarrow f_i(v_1 + \pi y_1, \ldots, v_n + \pi y_n)$ for $i = 1, \ldots, m$
13. $\quad$ FOR $w \in \text{IntegerPoints}(\mathrm{r} - 1, \mathrm{g}_1, \ldots, \mathrm{g}_\mathrm{m})$:
14. $\quad\quad$ Add $(v_1 + \pi w_1, \ldots, v_n + \pi w_n)$ to W
15. RETURN W

Obviously, if Y has some higher multiplicity $\mathcal{O}$-point, then succesive approximations to it will be in V_1 and never in V_0. The algorithm recurses infinitely. Therefore, if IntegerPoints gets called with $r \leq 0$, an error should be generated, indicating that the scheme Y has points that do not separate below the requested precision level. An alternative is to return such points as *non-separating* approximations to possible solutions and return them. These give the user neighbourhoods that could not be resolved at the requested precision.

It should also be clear, and this is an essential problem, that step 7 only tests that v is *approximately* on Y. While v can be uniquely lifted to arbitrary precision r' using $\{f_{i_1}, \ldots, f_{i_n}\}$ (provided the f_i themselves are given to sufficient precision), it may be that this lift does not satisfy the other equations to precision r', but that it did to precision r. Obviously, if Y is presented as a complete intersection and $n = m$, then this problem will not arise. Otherwise, the best one can do is to assume that the user supplies a sufficiently high r to begin with.

5.2 Determining solvability of complete intersections

Let $X \subset \mathbb{P}^n$ be a complete intersection defined over a number field K of dimension d. We assume that X is equidimensional, which means that its

maximal components are all of dimension d. This condition is certainly met if X is irreducible. Let X' denote the reduced singular subscheme.

Let L be the completion of K at some finite prime. First we assume $X'(L)$ is empty. In this case, our task is to decide if $X(L)$ contains any non-singular points. We follow the same approach as in Section 5.1 and note that, again, it is sufficient to solve the problem for integral points on affine complete intersections Y:

Algorithm HasNSIntegralPoints$(f_1, \ldots, f_{n-d})$:

1. $(f_1, \ldots, f_{n-d}) \leftarrow \text{Saturate}(f_1, \ldots, f_{n-d})$.
2. Let $V \subset \mathcal{O}^n$ be a set of representatives of the solutions of $\overline{f_1} = \cdots = \overline{f_{n-d}} = 0$ in $\mathcal{O}/\mathfrak{p}$.
3. IF any of the points in V represent a point over $\mathcal{O}/\mathfrak{p}$ with a d-dimensional tangent space:
4. RETURN *true*
5. FOR $v \in V$:
6. $g_i \leftarrow f_i(v_1 + \pi y_1, \ldots, v_n + \pi y_n)$ for $i = 1, \ldots, n-d$
7. IF HasNSIntegralPoints$(g_1, \ldots, g_{n-d})$:
8. RETURN *true*
9. RETURN *false*

Since we assume that Y is a complete intersection, the problem of step 7 in Section 5.1 does not arise.

The strategy to determine if $X(L)$ is empty is now straightforward:

Algorithm CIHasPoints(X, L):

1. if $X'(L)$ is nonempty, then $X(L)$ is nonempty
2. otherwise, use HasNSIntegralPoints on the affine patches of X to decide if $X(L)$ is nonempty.

Obviously, step 1 can only be decided if X' is of one of the types we have considered before, i.e., X' is empty, $\dim X' = 0$ or X' is a complete intersection. One may be able to show that $X'(L)$ is empty by showing that some complete intersection containing X' has no points over L, but the converse does not hold.

In order to compute X', it is essential that X is represented exactly over some field allowing exact arithmetic, because only then do Groebner basis algorithms allow for the computation of the radical of an ideal.

5.3 Solvability of smooth curves

In this section we consider a reduced scheme $X \subset \mathbb{P}^2$ given by a single equation $f(x, y, z) = 0$. We present an algorithm to determine the local solvability of the desingularisation $\tilde{X}$ of X. As in Section 5.2, we note that it is sufficient to solve the problem for integral points on affine curves $Y : f(x, y) = 0$ and to a large extent, the algorithm is the same. The only difference occurs

in how singular points in $Y(\mathcal{O})$ are treated. Instead of considering them as rational points, we blow up Y at the singularity and remove the exceptional component. We then look for L-valued points on the resulting scheme.

First, let us study how to blow up an affine curve in $(0,0)$. Therefore, let $f \in \mathcal{O}[x,y]$ describe a curve in $\mathbb{A}^2$ with a singularity at $(0,0)$ and no other $\mathcal{O}$-valued singularities. We resolve the singularity by blowing up $\mathbb{A}^2$ at $(0,0)$. This means we take the inverse image under

$$\begin{array}{rcl} \beta : \{xv = yu\} \subset \mathbb{P}^2 \times \mathbb{A}^2 & \to & \mathbb{A}^2 \\ (u:v;x,y) & \mapsto & (x,y) \end{array}$$

Note that any point $(u:v;x,y)$ that has an image $(x,y) \in \mathbb{A}^2(\mathcal{O})$ under β has a representative of one of the forms $(u:1;x,y)$ or $(1:\pi v;x,y)$ with $u,v \in \mathcal{O}$. Hence, any integral point on $\beta^{-1}Y$ is covered by an integral point on one of $\beta_1^{-1}Y$ or $\beta_2^{-1}Y$, where

$$\begin{array}{rcl} \beta_1 : \mathbb{A}^2 & \to & \mathbb{A}^2, \\ (u,y) & \to & (uy,y) \end{array} \qquad \begin{array}{rcl} \beta_2 : \mathbb{A}^2 & \to & \mathbb{A}^2, \\ (v,x) & \to & (x,\pi xv) \end{array}$$

To remove the exceptional component from $\beta_1^{-1}Y : f(uy,y) = 0$, compute

$$Y_1 : f_1(u,y) = f(uy,y)/u^{(\text{highest possible power})}.$$

The curve Y_1 may have new singularities, but since Y_1 is isomorphic to Y outside $u = 0$, any integral-valued singularities will have $u = 0$. The singular points of Y_1 can be easily described as

$$Y_1'(\mathcal{O}) = \left\{ (u,0) : u \in \mathcal{O} \text{ and } f_1(u,0) = \frac{\partial f_1}{\partial u}(u,0) = \frac{\partial f_1}{\partial y}(u,0) = 0 \right\}$$

and can be computed using univariate root finding for polynomials over $\mathcal{O}$. Of course, in practice, an expression like "$= 0$" should be interpreted as "is indistinguishable from 0 at the given precision". For $\beta_2^{-1}Y$ we can proceed similarly.

Given a list S of integral-valued singularities, one can check the desingularisation of $Y : f(x,y) = 0$ for integral points:

Algorithm HasSmoothIntegralPoints(f, S):

1. $f \leftarrow f/\pi^{\nu(f)}$
2. IF $S = \{(x_0,y_0)\}$:
3. $\quad f \leftarrow f(x+x_0, y+y_0)$
4. $\quad f_1 \leftarrow f(uy,y)/u^{(\text{highest possible power})}$
5. $\quad S_1 \leftarrow \left\{ (u,0) : u \in \mathcal{O} \text{ and } f_1(u,0) = \frac{\partial f_1}{\partial u}(u,0) = \frac{\partial f_1}{\partial y}(u,0) = 0 \right\}$
6. $\quad$ IF HasSmoothIntegralPoints(f_1, S_1): RETURN *true*
7. $\quad f_2 \leftarrow f(x,\pi xv)/v^{(\text{highest possible power})}$

8. $S_2 \leftarrow \left\{(v,0) : v \in \mathcal{O} \text{ and } f_2(v,0) = \frac{\partial f_2}{\partial v}(v,0) = \frac{\partial f_2}{\partial x}(v,0) = 0\right\}$
9. IF HasSmoothIntegralPoints(f_2, S_2): RETURN *true*
10. ELSE
11. Let $V \subset \mathcal{O}^2$ be a set of representatives of the solutions of $\overline{f} = 0$ in $\mathcal{O}/\mathfrak{p}$.
12. IF a point in V represents a nonsingular point over $\mathcal{O}/\mathfrak{p}$: RETURN *true*
13. FOR $(x_0, y_0) \in V$:
14. $g \leftarrow f(x_0 + \pi x, y_0 + \pi y)$
15. $S' \leftarrow \{((x_1 - x_0)/\pi, (y_1 - y0)/\pi) : (x_1, y_1) \in S\}$
16. Remove any non-integral entries from S'
17. IF HasSmoothIntegralPoints(g, S'): RETURN *true*
18. RETURN *false*

To determine local solvability of the desingularisation of a reduced projective plane curve $X \subset \mathbb{P}^2$, one can determine the reduced singular subscheme X' of X, find $X'(L)$ using Section 5.1 and apply HasSmoothIntegralPoints to each affine patch of X, using $X'(L)$ to initialise S.

5.4 Solvability of hyperelliptic curves

In this section, we adopt Magma's terminology and understand *hyperelliptic curve* to mean *nonsingular double cover of* $\mathbb{P}^1$. Some geometric hyperelliptic curves can be represented in this category (but not the ones that have a twisted $\mathbb{P}^1$ as a canonical model). Conics and some curves of genus 1 also fit in this category.

We represent such curves as a nonsingular curve in weighted projective space $\mathbb{P}_{(1,d,1)}$ with coordinates (x, y, z) and a model of the form

$$C : y^2 + h(x,z)y = f(x,z).$$

Over fields of odd characteristic we can complete the square and without loss of generality, we can assume $h = 0$. In this case, the nonsingularity of C means that $f(x,z)$ is a square-free form of degree $2d$ and a simple application of Riemann-Hurwitz shows that C is of genus $d-1$.

Of course, to decide if a hyperelliptic curve has points over L, one could cover it with two non-singular affine patches and use Section 5.3. One can also use [2, Appendix A.2], which is slightly more efficient. Both these algorithms are essentially polynomial in $\#\mathcal{O}/\mathfrak{p}$, though. We can do better if $\mathcal{O}/\mathfrak{p}$ is of odd characteristic and satisfies

$$(\#\mathcal{O}/\mathfrak{p}) - 2(d-1)\sqrt{\#\mathcal{O}/\mathfrak{p}} > 0.$$

We generalise an algorithm that is presented for $d = 2$ in [20] and [18]. It is based on the fact that a curve defined over a finite field of large cardinality compared to the genera of the components, must be *very* singular not to have any nonsingular rational points.

Since multiplying f with an even power of π does not change the local solvability of $y^2 = f(x,z)$, we can assume $f \in \mathcal{O}[x,z]$ with $0 \leq \nu(f) \leq 1$.

Note that if $\nu(f) = 0$, any point $(\overline{x} : \overline{y} : \overline{z}) \in \mathbb{P}_{(1,d,1)}(\mathcal{O}/\mathfrak{p})$ satisfying $\overline{y}^2 = \overline{f}(\overline{x},\overline{z})$ with $\overline{y} \neq 0$ or $(\overline{x} : \overline{z})$ a zero of $\overline{f}$ of multiplicity 1 is a nonsingular point on $\overline{C}$ and hence Hensel-lifts to a point in $C(L)$. If we can show such a point exists, then $C(L)$ is not empty. We distinguish the following cases.

1. $\nu(f) = 1$. If $x, z \in \mathcal{O}$ such that $f(x,z)$ is a square, then in particular, $\nu(f(x,z)) \equiv 0 \mod 2$. Hence, $\overline{(x : z)}$ must be a root of $\overline{f/\pi}$ in $\mathcal{O}/\mathfrak{p}$. For any such root we take a representative $(x_0, z_0) \in s\mathcal{O}^2$ and we test $y^2 = f(x_0+\pi x, z_0+\pi z)/\pi^2$ for local solvability. If any of those cases is solvable, then so is the original equation. If none is, or if no roots are avaliable, then $y^2 = f(x,z)$ has no solutions.

2. $\nu(f) = 0$ and $\overline{f} = \alpha(g(\overline{x},\overline{z}))^2$ with α a non-square in $\mathcal{O}/\mathfrak{p}$. If $x, z \in \mathcal{O}$ such that $f(x,z)$ is a square, then $g(\overline{x},\overline{z}) = 0$. Hence we take representatives $(x_0, z_0) \in \mathcal{O}^2$ for the roots of g and test $y^2 = f(x_0 + \pi x, z_0 + \pi z)$ for local solvability. If any of those cases is solvable, then so is the original equation. If none is, or if no roots are avaliable, then $y^2 = f(x,z)$ has no solutions.

3. $\nu(f) = 0$ and $\overline{f} = \alpha(g(\overline{x},\overline{z}))^2$ with α a nonzero square in $\mathcal{O}/\mathfrak{p}$. We take $(x_0, z_0) \in \mathcal{O}$ to represent a non-root of g in $\mathbb{P}^1(\mathcal{O}/\mathfrak{p})$. Note that g has at most d roots, while $\#\mathbb{P}^1(\mathcal{O}/\mathfrak{p}) = \#\mathcal{O}/\mathfrak{p} + 1 > 2(d-1)$ points, so this is easy. Then $f(x_0, z_0)$ is a square, because it represents a non-zero square in $\mathcal{O}/\mathfrak{p}$. Therefore, the original equation is solvable.

4. In all other cases, $\overline{f} = g_1(\overline{x},\overline{z})(g_2(\overline{x},\overline{z}))^2$, where g_1 is square-free and $\deg(g_1) + 2\deg(g_2) = 2d$. The curve $D : y_1^2 = g_1(\overline{x},\overline{z})$ is a hyperelliptic curve over $\mathcal{O}/\mathfrak{p}$ of genus $(\deg(g_1) - 2)/2$ and hence, by the Hasse-Weil bounds, has at least

$$(\#\mathcal{O}/\mathfrak{p}) - 2(d-1)\sqrt{\#\mathcal{O}/\mathfrak{p}} + (2\deg g_2 + 2)\sqrt{\#\mathcal{O}/\mathfrak{p}}$$

points. It follows that D must have points $(\overline{x}, y_1, \overline{z})$ with $g_2(\overline{x},\overline{z}) \neq 0$. Since the higher multiplicity roots of $\overline{f}$ are exactly the roots of g_2, it follows that $\overline{y}^2 = f(\overline{x},\overline{z})$ has a non-singular point, which is Hensel-liftable. It follows that $C(L)$ is non-empty.

These cases lead directly to a recursive algorithm, where the most difficult operation is factorisation of univariate polynomials of degree at most $2d$ over a finite field. The branching degree of the algorithm is bounded by $2d$ as well and not (as is the algorithm in Section 5.3), essentially by $\#\mathcal{O}/\mathfrak{p}$.

6 Mordell-Weil groups of Elliptic curves

The *Mordell-Weil group* of an abelian variety A over a number field K is the set of K-rational points $A(K)$. The abelian variety structure of A induces a group structure on $A(K)$. A celebrated theorem of Weil, which for elliptic curves over $\mathbb{Q}$ was already proved by Mordell, states that $A(K)$ is a finitely generated commutative group. Actually determining $A(K)$, even in the case where A is an elliptic curve and $K = \mathbb{Q}$, is still more an art than a science. However, even an artist works better if he has proper tools available. In this chapter, we introduce the tools that Magma offers to determine Mordell-Weil groups of elliptic curves over number fields. The Magma implementation is based on [3].

First, we review some of the fundamental definitions connected to the subject. We do not give much detail, since many other excellent descriptions already exist (see for instance [21]). Computational concerns that arise specifically when applying the methods outlined here to elliptic curves over number fields are addressed in [22].

Let E be an elliptic curve over a number field K. In order to bound the free rank of $E(K)$, we bound the size of $E(K)/2E(K)$. For this, we use the 2-*Selmer group* of E over K. From the exact Galois-cohomology sequence

$$0 \to E(K)/2E(K) \to H^1(K, E[2]) \to H^1(K, E)$$

we derive a set that approximates the image of $E(K)/2E(K)$ in $H^1(K, E[2])$ *everywhere locally*. We define $S^{(2)}(E/K)$ to be the intersection of the kernels of $H^1(K, E[2]) \to H^1(K_p, E)$ for *all* primes p of K:

$$0 \to S^{(2)}(E/K) \to H^1(K, E[2]) \to \prod_p H^1(K_p, E).$$

Clearly, $S^{(2)}(E/K)$ provides a sharp bound, unless $H^1(K, E[2])$ maps to any cocycle in $H^1(K, E)$ that trivialises under all restrictions $\mathrm{Gal}(K_p) \subset \mathrm{Gal}(K)$. The group consisting of such cocycles is called the *Shafarevich-Tate group* $Ш(E/K)$ and we have the exact sequence

$$0 \to E(K)/2E(K) \to S^{(2)}(E/K) \to Ш(E/K)[2] \to 0.$$

The group $S^{(2)}(E/K)$, as a Galois-module, can be represented in the following way (see [9]). For an elliptic curve

$$E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6,$$

we define the following algebra:

$$A[\theta] = K[X]/(X^3 + a_2X^2 + a_4X + a_6 + (a_1X + a_3)^2/4).$$

The Galois-module $H^1(K, E[2])$ can be identified with the subgroup of A^*/A^{*2} consisting of the elements of square norm and for some suitable, effectively

computable, set S of primes of K, we have $S^{(2)}(E/K) \subset A(2,S)$. The map $\mu : E(K) \to S^{(2)}(E/K)$ is induced by $(x,y) \mapsto x - \theta$ where $x - \theta \in A^*$.

Magma computes $S^{(2)}(E/K)$ by computing the local images of

$$E(K_p) \to A^*/A^{*2} \otimes K_p$$

and computing the elements from $A(2,S)$ of square norm that land in these local images. Wherever possible, elements of $A(2,S)$ are left in product representation, to avoid coefficient blowup.

As an example, we compute $S^{(2)}(E_d/K)$ for $d = 2\zeta^3 - 2\zeta^2 - 2$, as defined in Section 4.

```
> _<x>:=PolynomialRing(Rationals());
> K<zeta>:=NumberField(x^4-x^3+x^2-x+1);
> OK:=IntegerRing(K);
> d:=2*zeta^3-2*zeta^2-2;
> E<X,Y,Z>:=EllipticCurve([0,(-3*zeta^3-zeta+1)*d,0,(-zeta^2-zeta-1)*d^2,0]);
> two:=MultiplicationByMMap(E,2);
> mu,tor:=IsogenyMu(two);
> S2E,toS2E:=SelmerGroup(two);S2E;
Abelian Group isomorphic to Z/2 + Z/2 + Z/2 + Z/2
Defined on 4 generators in supergroup:
    S2E.1 = $.1 + $.2 + $.6 + $.7 + $.8 + $.9
    S2E.2 = $.2 + $.4 + $.7 + $.8
    S2E.3 = $.1 + $.2 + $.5 + $.7
    S2E.4 = $.3 + $.9
Relations:
    2*S2E.1 = 0
    2*S2E.2 = 0
    2*S2E.3 = 0
    2*S2E.4 = 0
```

So we see that $E(K)/2E(K) \subset (\mathbb{Z}/2\mathbb{Z})^4$. Part of this corresponds to the image of the torsion subgroup of E.

```
> Etors,EtorsMap:=TorsionSubgroup(E);
> sub<S2E|[toS2E(mu(EtorsMap(g))):g in OrderedGenerators(Etors)]>;
Abelian Group isomorphic to Z/2 + Z/2
Defined on 2 generators in supergroup S2E:
    $.1 = S2E.3 + S2E.4
    $.2 = S2E.1 + S2E.4
Relations:
    2*$.1 = 0
    2*$.2 = 0
Mapping from: Abelian Group isomorphic to Z/2 + Z/2
Defined on 2 generators in supergroup S2E:
    $.1 = S2E.3 + S2E.4
```

```
    $.2 = S2E.1 + S2E.4
Relations:
    2*$.1 = 0
    2*$.2 = 0 to GrpAb: S2E
```

We conclude that the free rank of $E(K)$ is at most 2. We look for rational points on E, up to some tiny bound and we see that the found points already generate $E(K)/2E(K)$.

```
> V:=MyRationalPoints(E,5);
> sub<S2E|[toS2E(mu(P)):P in V]> eq S2E;
true
```

We then select some minimal subset of V that generates $E(K)/2E(K)$ and construct a group homomorphism from an abstract abelian group into G.

```
> gs:=[E![0,0],
>      E![-2*zeta^3 - 2*zeta + 2,0],
>      E![-2*zeta^3,-4*zeta^2],
>      E![-2*zeta^3 - 4*zeta + 4,-4*zeta^3 + 4*zeta]];
> assert S2E eq sub<S2E|[toS2E(mu(g)):g in gs]>;
> G:=AbelianGroup([2,2,0,0]);
> mwmap:=map<G->E|g:->&+[c[i]*gs[i]:i in [1..#gs]] where c:=Eltseq(g)>;
```

In fact, we could have left this all to the system and just executed:

```
> success,G,mwmap:=PseudoMordellWeilGroup(E);
> assert success;
```

Here, it is of the utmost importance to check that `success` is `true`. Only then is there a guarantee that the returned group is of finite (odd) index in $E(K)$. If the value `false` is returned, then only a subgroup is returned that will itself be 2-saturated in $E(K)$ (meaning that, if $2P \in G$ and $P \in E(K)$ then $P \in G$ as well), but need not be of finite index.

In fact, the computation done by `PseudoMordellWeilGroup` is not completely equivalent to the computation we did above. By default, if possible, `PseudoMordellWeilGroup` uses a 2-*isogeny descent* (see [21]). For any non-trivial element of $E[2](K)$, there is an associated 2-*isogeny*

$$\phi : E \to E',$$

together with a dual isogeny $\hat{\phi} : E' \to E$, such that $\hat{\phi} \circ \phi = 2|_E$. In complete analogy to the 2-Selmer group, we define the ϕ-Selmer group by considering the exact sequence

$$0 \to E'(K)/\phi E(K) \to H^1(K, E[\phi]) \to H^1(K, E)$$

and we define $S^{(\phi)}(E/K)$ by insisting on exactness of

$$0 \to S^{(\phi)}(E/K) \to H^1(K, E[\phi]) \to \prod_p H^1(K_p, E).$$

From the exact sequence

$$0 \to E[\phi](K) \to E[2](K) \to E'[\hat{\phi}](K) \to \\ E'(K)/\phi E(K) \to E(K)/2E(K) \to E(K)/\hat{\phi}E'(K) \to 0$$

it follows that

$$4\#E(K)/2E(K) = \#E'(K)/\phi E(K) \cdot \#E(K)/\hat{\phi}E'(K) \cdot \#E[2](K).$$

Therefore, we can use ϕ-Selmer groups to bound the free rank of $E(K)$ as well. One can compute ϕ-Selmer groups in the same way as 2-Selmer groups.

```
> phi:=TwoIsogeny(E![0,0]);
> Sphi,toSphi:=SelmerGroup(phi);
> phihat:=DualIsogeny(phi);
> Sphihat,toSphihat:=SelmerGroup(phihat);
> 4*#S2E, #Sphi, #Sphihat, #TwoTorsionSubgroup(E);
64 2 8 4
```

Apart from providing an upper bound on the rank of $E(K)$, Selmer groups also contain information about possible generators of $E(K)$. To access this information, it is useful to interpret $S^{(2)}(E/K) \subset H^1(K, E[2])$ as a set of twists of the cover $E \xrightarrow{2} E$. The second return value of `IsogenyMu` gives a map that computes such a cover from an element of $H^1(K, E[2])$. The covering space is represented as an intersection X of two quadrics in $\mathbb{P}^3$, with a map $\phi : X \to E$. If the cover represents an element from $S^{(2)}(E/K)$, however, one can construct a model of X of the form $C : v^2 = f_0u^4 + \cdots + f_4$. A call to `Quartic` realises this.

```
> delta:=S2E.2;
> psi:=tor(delta@@toS2E);
> XX:=Domain(psi);
> C,CtoXX:=Quartic(XX);
```

One can then search for points on C, which can be mapped back to E.

```
> V:=MyRationalPoints(C,10);
> assert #V gt 0;
> P:=psi(CtoXX(Rep(V)));P;
(-zeta^3 - 4*zeta^2 - 2*zeta - 2 : -14*zeta^3 + zeta^2 - 6*zeta + 10 : 1)
> assert delta eq toS2E(mu(P));
```

Note, however, that it is a rarity for it to make sense to search for points on C as computed. The model computed for C generallly does not have particulary small coefficients and there is no reason to expect that the point we are looking for will be easier to find on C than on E. Over $\mathbb{Q}$, a rather satisfactory solution to this problem has been found in the form of a proper minimization and reduction theory [24], [12]. For other number fields, a satisfactory theory

is woefully lacking and Magma leaves it to the art and ingenuity of the user to find a suitable model from the returned one.

The same functionality is available for 2-isogenies as well. Here, the cover corresponding to an element in the Selmer group naturally has a model of the form $C : v^2 = f_0u^4 + f_2u^2 + f_4$, and therefore it does make sense to look for rational points on the covering curve. Therefore, the routine `PseudoMordellWeilGroup` uses the following default strategy:

1. If a 2-isogeny is available, this is chosen as isogeny ϕ, Otherwise full multiplication-by-2 is used as ϕ.
2. The ϕ-Selmer group is computed and, if $\phi \neq 2$, then also the $\hat{\phi}$-Selmer group is computed.
3. The image of the torsion subgroup is determined in the computed Selmer groups.
4. The elliptic curve is searched for rational points up to a preset bound and, if relevant, also the 2-isogenous curve is searched. If the found points already generate the Selmer group(s), we are done.
5. Otherwise, if ϕ is a 2-isogeny or if the elliptic curve is defined over $\mathbb{Q}$, the covers corresponding to elements of the Selmer group that are not represented by rational points are constructed (and, if reduction is available, reduced) and searched for points.
6. If this still leaves some elements of the Selmer group(s) not corresponding to found rational points, then `false` is returned, together with the group generated by the found points. Otherwise, `true` is returned.

One can override the default choice of isogeny and whether or not homogeneous spaces should be used for searching for rational points.

If $Ш(E/K)[2]$ is nontrivial, then obviously neither a 2-descent nor a 2-isogeny descent will provide a sharp bound on $E(K)/2E(K)$. In this situation, a 4-descent may give more information ([18] and [25]). For $K = \mathbb{Q}$, Tom Womack has implemented routines to perform such a computation in MAGMA. Another option consists of using the Cassels-Tate pairing to obtain more information (see [10]).

Alternatively, one may use *visualisation* (see [13]) to obtain more information. See [7] for an explicit approach using MAGMA.

7 Chabauty methods using elliptic curves

In this section, we show how, given an elliptic curve E over a number field K and a map $u : E \to \mathbb{P}^1$, one can try to determine $\{p \in E(K) : u(p) \in \mathbb{P}^1(\mathbb{Q})\}$. The method is an adaptation of Chabauty's partial proof of Mordell's conjecture [11] and is described in [5] and [2]. A similar method applied to bielliptic genus 2 curves is described in [16]. We quickly review the theory here.

We write $\mathcal{O}$ for the ring of integers of K. and we fix models of E and $\mathbb{P}^1$ over $\mathcal{O}$. We choose a prime p such that the primes $\mathfrak{p}_1, \ldots, \mathfrak{p}_t$ of K over p are unramified and such that the cover $u : E \to \mathbb{P}^1$ has good reduction at each $\mathfrak{p}_i$, as a scheme morphism over $\mathcal{O}$.

Let p be a rational prime which is unramified in K. Let $\mathfrak{p}_1, \ldots, \mathfrak{p}_t$ be the primes of K over p. Suppose that $u : E \to \mathbb{P}^1$ has good reduction at all $\mathfrak{p}_i$. We write $\mathcal{O}$ for the ring of integers of K, $E(\mathcal{O}/\mathfrak{p}_i)$ for the points in the special fibre of E, considered as a scheme over $\mathcal{O}_{\mathfrak{p}_i}$ and $E^{(1)}(K_{\mathfrak{p}_i})$ for the kernel of reduction:

$$0 \to E^{(1)}(K_{\mathfrak{p}_i}) \to E(K_{\mathfrak{p}_i}) \xrightarrow{\rho_i} E(\mathcal{O}/\mathfrak{p}_i) \to 0$$

Let $g_1, \ldots, g_r \in E(K)$ be generators of the free part of $E(K)$. Then if $P_0 = T + n_1 g_1 + \cdots + n_r g_r \in E(K)$ has $u(P_0) \in \mathbb{P}^1(\mathbb{Q})$, then certainly (abusing notation), $u(\rho_i(P_0)) \in \mathbb{P}^1(\mathbb{F}_p)$ and in fact $u(\rho_i(P_0)) = u(\rho_j(P_0))$. The points $P_0 \in E(K)$ define a collection of cosets of

$$\Lambda_p = \bigcap_{i=1}^{t} \left(E(K) \cap E^{(1)}(K_{\mathfrak{p}_i}) \right)$$

Let V_p be this coset collection and let $b_1, \ldots, b_r$ be generators of Λ_p. In Magma, both V_p and Λ_p are easily computed.. We take the the same elliptic curve as in the previous chapter, together with its (finite index subgroup of the) Mordell-Weil group and the cover suggested in Section 4.

```
> P1:=ProjectiveSpace(Rationals(),1);
> u:=map<E->P1|[-X + (zeta^3 - 1)*d*Z,X+(-zeta^3-zeta)*d*Z]>;
> V3:=RelevantCosets(mwmap,u,Support(3*OK));
> Lambda3:=Kernel(V3[1]);
> GmodLambda3:=Codomain(V3[1]);
> V3;
<Mapping from: GrpAb: G to GrpAb: GmodLambda3, {
    0,
    11*GmodLambda3.2,
    GmodLambda3.2,
    GmodLambda3.1 + 10*GmodLambda3.2,
    5*GmodLambda3.2,
    7*GmodLambda3.2,
    GmodLambda3.1 + 2*GmodLambda3.2
}>
```

As is clear, the coset data is returned as a tuple consisting of the map $G \to G/\Lambda_p$, together with the collection of cosets, represented as elements of G/Λ_p. We can compute a similar coset collection V_q and intersect it with V_p. This gives a new coset collection mod $\Lambda_p + \Lambda_q$. Alternatively, one could project $V_p \cap V_q$ down to get again a coset collection modulo Λ_p. This is what in Magma is called a `Weak` coset intersection.

```
> V11:=RelevantCosets(mwmap,u,Support(11*OK));
> V3i11:=CosetIntersection(V3,V11:Weak);
> V3i11;
<Mapping from: GrpAb: G to GrpAb: GmodLambda3, {
    0,
    11*GmodLambda3.2,
    GmodLambda3.2,
    5*GmodLambda3.2,
    7*GmodLambda3.2
}>
```

In order to bound the number of points $P \in E(K)$ with $u(P) \in \mathbb{P}^1(\mathbb{Q})$, we make use of the formal group description of the group structure on E. Let $b_1, \ldots, b_r$ be generators of $\Lambda_p \subset E(K)$. In terms of formal power series, there are isomorphisms

$$\mathrm{Exp}_E : K[[z]] \to E(K[[z]]), \mathrm{Log}_E : E(K[[z]]) \to K[[z]],$$

where z is a local coordinate on E around the origin. These power series converge on $E^{(1)}(K_{\mathfrak{p}})$ for unramified primes of odd residue characteristic and establish an isomorphism $E^{(1)}(K_{\mathfrak{p}}) \simeq \mathfrak{p}\mathcal{O}_{\mathfrak{p}}$. Therefore, for each prime $\mathfrak{p}_i$ we obtain a power series

$$\theta_{P_0,i}(n_1, \ldots, n_r) = u\left(P_0 + \mathrm{Exp}_E\left(\sum_{j=1}^{r} n_j \mathrm{Log}_E(b_j)\right)\right) \in \mathcal{O}_{\mathfrak{p}_i}[[n_1, \ldots, n_r]].$$

If $u(P_0 + n_1 b_1 + \cdots + n_r b_r)$, then $\theta_{P_0,i}(n_1, \ldots, n_r) \in \mathbb{Q}_p$ and $\theta_{P_0,i}(n_1, \ldots, n_r) = \theta_{P_0,j}(n_1, \ldots, n_r)$. Using that $\mathcal{O}_{\mathfrak{p}_i}$ is a finite $\mathbb{Z}_p$-module, we can decompose

$$\mathcal{O}_{\mathfrak{p}_i}[[n_1, \ldots, n_r]] = \oplus \mathbb{Z}_p[[n_1, \ldots, n_r]]$$

and express the above equations as $[K : \mathbb{Q}] - 1$ equations in $\mathbb{Z}_p[[n_1, \ldots, n_r]]$. We can do this in Magma:

```
> P0:=mwmap(G.3+G.4);
> u(P0);
(-3 : 1)
> theta:=ChabautyEquations(P0,u,mwmap,Support(3*OK));
> PrintToPrecision(theta[1],1);"";PrintToPrecision(theta[2],1);"";PrintToPrecision(theta
O(3^5) - (3 + O(3^5))*$.1 + (3^2*10 + O(3^5))*$.2
O(3^5) - (3*29 + O(3^5))*$.1 - (3*32 + O(3^5))*$.2
O(3^5) - (3^2*5 + O(3^5))*$.1 - (3^4 + O(3^5))*$.2>
```

A consequence of the shape of $\mathrm{Exp}_E(z)$ is that the power series returned by `ChabautyEquations` have the property that the coefficient c of a monomial of total degree d satisfies $\mathrm{ord}_p(c) \geq d - \lfloor \mathrm{ord}_p(d!) \rfloor$. In particular, from the

power series above, one can see that any integral solution (n_1, n_2) must satisfy $n_1 \equiv n_2 \equiv 0 \mod 3$ and, since

$$\det \begin{pmatrix} -1 & 0 \\ -29 & -32 \end{pmatrix} \not\equiv 0 \mod 3,$$

by Hensel's lemma such an integral solution lifts uniquely to $(0,0)$. In other words, there is at most one point in the coset $G_3+G_4+\Lambda_3$ that has a rational image under u. One can do similar arguments for the other fibres of reduction:

```
> N,V,R,C:=Chabauty(mwmap,u,3:Aux:={7});
> assert N eq #V;
> assert #C[2] eq 0;
> R;
4
> V;
{
    0,
    G.3 - G.4,
    -G.3 + G.4,
    G.3 + G.4,
    -G.3 - G.4
}
> {EvaluateByPowerSeries(u,mwmap(P)):P in V};
{ (-1 : 1), (-1/3 : 1), (-3 : 1) }
```

To interpret the above results, consider that in the previous computations, we have not really used that we have generators of $E(K)$. In fact, for this particular example, we don't know we have. We only know we have generators of some finite odd index subgroup G. For the finite field arguments, we only need that the $[E(K) : G]$ is prime to $[E(\mathcal{O}/\mathfrak{p}_i) : \rho_i(G)]$ for each of the i. Since the power series argument works for $n_1, n_2 \in \mathbb{Z}_p$, we only need that that $[E(K) : G]$ is prime to p as well. However, when computing $\mathrm{Log}_E(b_j)$, we can often already deduce that $p \nmid [E(K) : G]$.

We only need G to be q-saturated in $E(K)$ for finitely many l. The l that are encountered during the computations, are collected as prime divisors of `R`. In our case, this is only 2 and since we already know G to be 2-saturated in $E(K)$, any conclusions we draw from G will also be valid for $E(K)$. The interpretation of the other return values can be stated as follows.

$$\#\{P \in E(K) : u(P) \in \mathbb{P}^1(\mathbb{Q})\} \leq \mathtt{N}$$

$$\mathtt{V} \subset \{P \in E(K) : u(P) \in \mathbb{P}^1(\mathbb{Q})\} \subset \mathtt{V} \cup \mathtt{C}$$

Here, `C` is a coset collection of the type we described before. Note that if $\#\mathtt{V} = \mathtt{N}$ then all inequalities above are identities.

The routine `Chabauty` only tries a limited number of techniques to determine p-adic solution and only with finite precision. It uses an adaptation

of the algorithm in Section 5.1 to find solutions of multiplicity 1 and it uses a generalisation of [2, Lemma 4.5.1] to test if the solution $(0, \ldots, 0)$ is the only integral solution of possibly higher multiplicity. It may therefore fail to produce a finite bound at all. In that case, $\mathtt{N} = \infty$ is returned.

As an advanced example, we also give the computation for $d = -3\zeta^3 - 7\zeta^2 - 8\zeta - 9$.

```
> d:=-3*zeta^3-7*zeta^2-8*zeta-9;
> E<X,Y,Z>:=EllipticCurve([0,(-3*zeta^3-zeta+1)*d,0,(-zeta^2-zeta-1)*d^2,0]);
> P1:=ProjectiveSpace(Rationals(),1);
> u:=map<E->P1|[-X + (zeta^3 - 1)*d*Z,X+(-zeta^3-zeta)*d*Z]>;
> success,G,mwmap:=PseudoMordellWeilGroup(E);
> assert success;
> [mwmap(P):P in OrderedGenerators(G)];
[ (-41*zeta^3 + 18*zeta^2 - 14*zeta + 42 : 0 : 1), (0 : 0 : 1), (-5*zeta^3 + 6*zeta^2 + 9
    -69*zeta^3 + 17*zeta^2 - 34*zeta + 60 : 1), (-6*zeta^3 + 3*zeta^2 - zeta + 6 : 57*zet
    16*zeta^2 + 27*zeta - 51 : 1), (-36*zeta^3 + 8*zeta^2 - 20*zeta + 32 : 10*zeta^3 + 72
    60*zeta + 62 : 1) ]
> N,V,R,C:=Chabauty(mwmap,u,3);
> C31,R31:=RelevantCosets(mwmap,u,Support(31*OK));
> R:=LCM(R,R31);
> Cnew:=CosetIntersection(C,C31:Weak);
> assert #Cnew[2] eq 0;
> R;
2
> V;
{
    0,
    G.4 - G.5,
    -G.4 + G.5
}
> {EvaluateByPowerSeries(u,mwmap(P)):P in V};
{ (3/2 : 1), (-1 : 1) }
```

An interesting feature of this example is, that the 3-adic argument by itself is not sufficient. We see that there are two 3-adic "ghost" solutions. The 3-adic computation did come up with a rather precise 3-adic approximation of these putative solutions. The cosets are disjoint from V_{31}, so we proved that they indeed only correspond to $\mathbb{Z}_3$-solutions and not rational ones.

Incidentally, specifying 31 as an "auxiliary" prime, such that V_3 and V_{31} get intersected before the 3-adic argument, would have solved this particular equation as well, as would 191 by itself.

The other 3 values of d mentioned in Section 4 can be solved in a similar way, either with $p = 31$ or $p = 191$.

8 The equations $x^n + y^n = Dz^2$ for $n = 6, 7, 9, 11, 13, 17$

The proof of Theorem 2 for the remaining cases is straightforward and, in many cases, easier than for $n = 5$, because there are no non-trivial solutions. For each n, we outline a successful strategy. For full details, we refer the reader to the accompanying electronic resource [6].

$x^6 + y^6 = Dz^2$: Since 6 is even, we can reduce the genus (and the number) of the curves to consider tremendously. Note that a solution with $y \neq 0$ corresponds to a rational point on the genus 2 curve $Y^2 = DX^6 + D$. For $D \in \{2, 3, 5, 6, 10, 11, 13, 17\}$, we conclude that only for $D = 2$ does this curve have points over $\mathbb{Q}_2$ and $\mathbb{Q}_7$. Following the same approach as in [4], we write $2X^6 + 2 = (2X^2 + 2)(X^4 - X^2 + 1)$ and we conclude that any point (X, Y) corresponds to a solution (X, Y_1, Y_2) of

$$dY_1^2 = 2X^2 + 2,\ dY_2^2 = X^4 - X^2 + 1$$

for $d \in \mathbb{Q}(2, \{2, 3\})$. Only for $d = 1$ does this system of equations have solutions over $\mathbb{Q}_2$. The curve $Y_2^2 = X^4 - X^2 + 1$ only has rational points with $X \in \{-1, 0, 1, \infty\}$.

$x^7 + y^7 = Dz^2$: We note that any solution corresponds to a solution to

$$C_d : Y^2 = d(X^6 - X^5 + X^4 - X^3 + X^2 - X + 1)$$

for some $d \in \mathbb{Q}(2, S)$, where S contains the prime divisors of $7D$. For the relevant values of D, only $d = 1, 7$ yield curves with points over $\mathbb{R}, \mathbb{Q}_2, \mathbb{Q}_7, \mathbb{Q}_{11}$.
With [23] it is straightforward to check that $\mathrm{Jac}(C_7)(\mathbb{Q})$ is of free rank 1 and using Stoll's implementation of [17], (3-adically), one finds that all rational points have $X = -1$.
For C_1, one uses [5] and the techniques outlined in Section 7 to show that all rational points have $X \in \{-1, 0, 1, \infty\}$

$x^9 + y^9 = Dz^2$: We factor:

$$\begin{aligned} y_1^2 &= d_1(x^6 - x^3z^3 + z^6) \\ y_2^2 &= d_2(x^2 - xz + z^2) \\ y_3^2 &= Dd_1d_2(x + 1) \end{aligned}$$

and note that any primitive solution (x, y, z) gives rise to a solution of the system above for $d_1, d_2 \in \mathbb{Q}(2, S)$, where S contains the prime divisors of $3D$. Furthermore, because $\gcd(x, z) = 1$, we have $\gcd(d_1, d_2) \mid 3$.
We can dehomogenize the first two equations and if we test them for simultaneous solvability over $\mathbb{R}, \mathbb{Q}_2, \mathbb{Q}_3, \mathbb{Q}_5$, we are only left with $d_1 \in \{1, 3\}$. The first equation gives rise to a curve of genus 2 with a Mordell-Weil group of free rank 1. Again, [17] yields that all points have $X \in \{-1, 1, 0, \infty\}$.

$x^{11} + y^{11} = Dz^2$: Using the same argument as for $n = 7$, we find all that solutions correspond to rational points on

$$C_d : Y^2 = d(X^{10} - X^9 + \cdots - X + 1)$$

for $d \in \{1, 11\}$. Rather than applying [8] to C_d directly, we substitute $(U, V) = ((X^2 + 1)/X, Y + Y/X)$ to find the covered curve

$$D_d : V^2 = d(U^6 + U^5 - 6U^4 - 5U^3 + 9U^2 + 5U - 2).$$

For $d = 1$ the free rank of the Mordell-Weil group is bounded above by 2 and for $d = 11$ the free rank is bounded by 1, but we could not find a generator. Using the techniques from [5], we find that $U(D_1(\mathbb{Q})) \subset \{-2, -1, 2, \infty\}$ and that $U(D_{11})(\mathbb{Q})) \subset \{-2, -1, 1, 2, \infty\}$. From this, it follows easily that C_d only has rational points above $X \in \{-1, 0, 1, \infty\}$ for $d = 1, 11$.

$x^{13} + y^{13} = Dz^2$: Using the same argument as for $n = 7$, we find that all solutions correspond to rational points on

$$C_d : Y^2 = d(X^{12} - X^9 + \cdots - X + 1)$$

for $d \in \{1, 13\}$. For $d = 13$ we substitute $(U, V) = ((X^2 + 1)/X, Y/X^3)$ to obtain

$$D_d : V^2 = 13(U^6 - U^5 - 5U^4 + 4U^3 + 6U^2 - 3U - 1).$$

Following [17] yields that $U(D_{13}(\mathbb{Q})) \subset \{-2\}$, which corresponds to $X = -1$.
For $d = 1$ we get a bound on the Mordell-Weil rank of 2, so we use that over $\mathbb{Q}(\beta)$ with $\beta^3 - \beta^2 - 4\beta + 1 = 0$, we have a quartic factor

$$X^4 + \beta X^3 + (\beta^2 + \beta - 1)X^2 + \beta X + 1$$

of $(X^{13} + 1)/(X + 1)$. Using [8] and [5] we find $X(C_1(\mathbb{Q})) \subset \{0, 1, \infty\}$.

$x^{17} + y^{17} = Dz^2$: Using the same argument as for $n = 7$, we find that all solutions correspond to rational points on

$$C_d : Y^2 = d(X^{16} - X^9 + \cdots - X + 1)$$

for $d \in \{1, 17\}$. Over $K = \mathbb{Q}(\beta)$ with $\beta^4 + \beta^3 - 6\beta^2 - \beta + 1 = 0$ we have

$$R(X) := X^4 + \beta X^3 + 1/2(-\beta^3 + 6\beta + 1)X^2 + \beta X + 1$$

with $N_{K/\mathbb{Q}}R(X) = (X^{17} + 1)/(X + 1)$. Hence, any rational point on C_d has an X-coordinate corresponding to a rational point on

$$D_\delta : V^2 = \delta R(X).$$

for some $\delta \in K(2,S)$ with $dN_{K/\mathbb{Q}}(\delta)$ a square, where S contains the primes above $2 \cdot 17 \cdot \delta$.
Local arguments show that only $\delta = 1, \beta^3+2\beta^2-3\beta+1$ need consideration. The techniques from Section 7 then show that $X(C_d(\mathbb{Q})) \subset \{-1,0,1,\infty\}$ for $d = 1, 17$.

References

1. Michael A. Bennett and Chris M. Skinner. Ternary Diophantine equations via Galois representations and modular forms. *Canad. J. Math.*, 56(1):23–54, 2004.
2. N. R. Bruin. *Chabauty methods and covering techniques applied to generalized Fermat equations*, volume 133 of *CWI Tract*. Stichting Mathematisch Centrum Centrum voor Wiskunde en Informatica, Amsterdam, 2002. Dissertation, University of Leiden, Leiden, 1999.
3. Nils Bruin. Algae, a program for 2-selmer groups of elliptic curves over number fields. see `http://www.cecm.sfu.ca/~bruin/ell.shar`.
4. Nils Bruin. The diophantine equations $x^2 \pm y^4 = \pm z^6$ and $x^2 + y^8 = z^3$. *Compositio Math.*, 118:305–321, 1999.
5. Nils Bruin. Chabauty methods using elliptic curves. *J. Reine Angew. Math.*, 562:27–49, 2003.
6. Nils Bruin. Transcript of computations. available from `http://www.cecm.sfu.ca/~bruin/nn2`, 2003.
7. Nils Bruin. Visualising Sha[2] in abelian surfaces. *Math. Comp.*, 73(247):1459–1476 (electronic), 2004.
8. Nils Bruin and E. Victor Flynn. Towers of 2-covers of hyperelliptic curves. Technical Report PIMS-01-12, PIMS, 2001. `http://www.pims.math.ca/publications/#preprints`.
9. J.W.S. Cassels. Diophantine equations with special reference to elliptic curves. *J. London Math. Soc.*, 41:193–291, 1966.
10. J.W.S. Cassels. Second descents for elliptic curves. *J. Reine Angew. Math.*, 494:101–127, 1998. Dedicated to Martin Kneser on the occasion of his 70th birthday.
11. Claude Chabauty. Sur les points rationnels des variétés algébriques dont l'irrégularité est supérieure à la dimension. *C. R. Acad. Sci. Paris*, 212:1022–1024, 1941.
12. J. E. Cremona. Reduction of binary cubic and quartic forms. *LMS J. Comput. Math.*, 2:64–94 (electronic), 1999.
13. John E. Cremona and Barry Mazur. Visualizing elements in the Shafarevich-Tate group. *Experiment. Math.*, 9(1):13–28, 2000.
14. Henri Darmon and Andrew Granville. On the equations $z^m = F(x,y)$ and $Ax^p + By^q = Cz^r$. *Bull. London Math. Soc.*, 27(6):513–543, 1995.
15. Claus Fieker. p-Selmer groups of number fields. Private communication.
16. E. Victor Flynn and Joseph L. Wetherell. Finding rational points on bielliptic genus 2 curves. *Manuscripta Math.*, 100(4):519–533, 1999.
17. E.V. Flynn. A flexible method for applying chabauty's theorem. *Compositio Mathematica*, 105:79–94, 1997.
18. J. R. Merriman, S. Siksek, and N. P. Smart. Explicit 4-descents on an elliptic curve. *Acta Arith.*, 77(4):385–404, 1996.

19. Bjorn Poonen and Edward F. Schaefer. Explicit descent for jacobians of cyclic covers of the projective line. *J. reine angew. Math.*, 488:141–188, 1997.
20. Samir Siksek. *Descent on curves of genus 1.* PhD thesis, University of Exeter, 1995.
21. Joseph H. Silverman. *The Arithmetic of Elliptic Curves.* GTM 106. Springer-Verlag, 1986.
22. Denis Simon. Computing the rank of elliptic curves over number fields. *LMS J. Comput. Math.*, 5:7–17 (electronic), 2002.
23. Michael Stoll. Implementing 2-descent for Jacobians of hyperelliptic curves. *Acta Arith.*, 98(3):245–277, 2001.
24. Michael Stoll and John E. Cremona. Minimal models for 2-coverings of elliptic curves. *LMS J. Comput. Math.*, 5:220–243 (electronic), 2002.
25. Tow Womack. *Four descent on elliptic curves over Q.* PhD thesis, University of Nottingham, 2003.

Index