TalkSTNB19

January 24, 2019

NOTE: In order to run the `Magma` commands below, the system needs to have a working copy of `Magma` installed.

The code has been tested with Version 2.24-3.

1 Mordell-Faltings a la Chabauty-Kim

1.1 Talk 2: Variations on the method of Coleman-Chabauty

Marc Masdeu

STNB 2019, January 23, 2019

```
In [1]: SetSeed(12314);
        _<x> := PolynomialRing(Rationals());
        P1:=ProjectiveSpace(Rationals(),1);
```

Let $X/\mathbb{Q}$ be a (smooth, projective) curve defined over $\mathbb{Q}$, of genus $g \geq 2$.

Goal: compute $X(\mathbb{Q})$.

1. Find a set $X_{\text{rat}} \subset X(\mathbb{Q})$ which be believe contains all the rational points.
2. Prove that this is indeed the case.

As has already been mentioned, (1) is usually done by enumerating points of small height.

So we will concentrate in (2). We assume that $X_{\text{rat}} \neq \emptyset$ (otherwise, see yesterday's talk by Francesc Bars).

1.2 Chabauty-Coleman

Idea: Embed the curve in an abelian variety, and the extra structure may help us on computing the points.

1.2.1 Easiest case: Jacobian is torsion

If $J(\mathbb{Q}) = \text{Jac}(X)(\mathbb{Q})$ has rank 0 and we can determine its torsion, then we only need to determine which points in $J(\mathbb{Q})$ come from $X(\mathbb{Q})$, and we are done. So we will suppose that $J(\mathbb{Q})$ is infinite.

1.2.2 An idea that doesn't work

Idea: consider $J(\mathbb{R})$ as a Lie group.

Then $X(\mathbb{Q}) \subseteq \overline{J(\mathbb{Q})} \cap X(\mathbb{R})$. If $\overline{J(\mathbb{Q})}$ is a proper subvariety inside $J(\mathbb{R})$, then it will intersect the curve $X(\mathbb{R})$ at finitely many points, which we may try to determine.

The above doesn't work because $J(\mathbb{Q})$ is typically dense in $J(\mathbb{R})^0$...

1.2.3 Chabauty

Chabauty's idea: replace $\mathbb{R}$ with $\mathbb{Q}_p$.

For simplicity, let p be a prime of good reduction for X. Then $J^1(\mathbb{Q}_p) = \ker(J(\mathbb{Q}_p) \to J(\mathbb{F}_p))$ is isomorphic to $\bigoplus_g \mathbb{Z}_p$.

If $\mathrm{rk}_{\mathbb{Z}} J(\mathbb{Q}) = r$, then $\overline{J(\mathbb{Q})}$ has dimension at most r inside $J(\mathbb{Q}_p)$.

Therefore if $r < g = \dim J$ then $\overline{J(\mathbb{Q})}$ has codimension ≥ 1, and we can expect $X(\mathbb{Q}_p)$ to intersect it at finitely many points.

Theorem (Chabauty 1941, Coleman 1985): If $r < g$, then $X(\mathbb{Q}_p) \cap \overline{J(\mathbb{Q})}$ is finite, and hence $X(\mathbb{Q})$ is finite.

To carry it out in practice, one finds a differential form $\omega \in H^0(J, \Omega^1)$ such that

$$\int_D \omega = 0 \quad \forall [D] \in J(\mathbb{Q}) \quad \text{(can be done since dim } H^0(J, \Omega^1) = g > r\text{)}.$$

Then one writes a power series $I(t)$ describing the above integral, and bounds $X(\mathbb{Q})$ by looking at the zeros of $I(t)$ (which are finite).

The `Magma` implementation combines this with the Mordell-Weil sieve to rule out "phantom" points, p-adic points that don't come from a rational point.

1.2.4 A prototypical example

$$y^2 = x^6 + 8x^5 + 22x^4 + 22x^3 + 5x^2 + 6x + 1.$$

```
In [2]: f:=x^6 + 8*x^5 + 22*x^4 + 22*x^3 + 5*x^2 + 6*x +1;
        X := HyperellipticCurve(f);
        X;
```

```
Hyperelliptic Curve defined by y^2 = x^6 + 8*x^5 + 22*x^4 + 22*x^3 + 5*x^2 + 6*x
    + 1 over Rational Field
```

We look for points of small height.

```
In [3]: print "Points of X at infinity: ", PointsAtInfinity(X);
        Xrat := Points(X : Bound:=10000);
        print "Set of easily found rational points of X:", Xrat;
        uX := map<X -> P1 | [X.1, X.3]>;
        print "Set of x-coordinates: ", {uX(P) : P in Xrat};
```

```
Points of X at infinity:  {@ (1 : -1 : 0), (1 : 1 : 0) @}
Set of easily found rational points of X: {@ (1 : -1 : 0), (1 : 1 : 0), (0 : -1
: 1), (0 : 1 : 1), (-3 : -1 : 1), (-3 : 1 : 1) @}
Set of x-coordinates:  { (-3 : 1), (1 : 0), (0 : 1) }
```

1.3 Goal: to prove that these are all the points of X

Compute $\mathrm{Jac}(X)$ and bound its rank.

```
In [4]: J := Jacobian(X);
        RankBound(J);
```

```
1
```

Define a nontorsion point in $J(\mathbb{Q})$.

```
In [5]: S := Setseq(Xrat);
        D := J![S[1], S[2]];
        D;
        print "Order of D is: ", Order(D);
```

```
(1, -x^3 - 4*x^2, 2)
Order of D is:  0
```

Note that 0 is Magma's way of saying ∞.
We can thus use Magma's Chabauty function.

```
In [6]: Chab := Chabauty(D);
        Chab;
```

```
{ (-3 : -1 : 1), (0 : -1 : 1), (-3 : 1 : 1), (0 : 1 : 1), (1 : -1 : 0), (1 : 1 :
0) }
```

```
In [7]: Chab eq Xrat;
```

```
true
```

1.4 Elliptic Chabauty

The previous approach has two drawbacks: 1. If g is "large" (> 2) it's hard to compute with $\mathrm{Jac}(X)$. 2. It won't work when $r \geq g$.

1.5 Example: a bielliptic curve.

$$X: \quad y^2 = (x^2+1)(x^4+1)$$

```
In [10]: f:=(x^2+1)*(x^4+1);
         X := HyperellipticCurve(f);
         print "Points of X at infinity: ", PointsAtInfinity(X);
         Xrat := Points(X : Bound:=10000);
         print "Set of easily found rational points of X:", Xrat;
         uX := map<X -> P1 | [X.1, X.3]>;
         print "Set of x-coordinates: ", {uX(P) : P in Xrat};
```

```
Points of X at infinity:  {@ (1 : -1 : 0), (1 : 1 : 0) @}
Set of easily found rational points of X: {@ (1 : -1 : 0), (1 : 1 : 0), (-1 : -2
: 1), (-1 : 2 : 1), (0 : -1 : 1), (0 : 1 : 1), (1 : -2 : 1), (1 : 2 : 1) @}
Set of x-coordinates:  { (1 : 1), (1 : 0), (-1 : 1), (0 : 1) }
```

```
In [11]: J := Jacobian(X);
         RankBound(J);
```

```
2
```

In fact, J it can be checked that the rank is indeed 2...

1.5.1 An elementary argument

Write $x = X/Z$ and $y = Y/Z^3$ with X, Y, Z sharing no common factors. Obtain

$$Y^2 = (X^2 + Z^2)(X^4 + Z^4).$$

Let $p > 2$ be such that $p \mid X^2 + Z^2$ and $p \mid X^4 + Z^4$. Then:

$$Z^2 \equiv -X^2 \pmod{p}, \quad Z^4 \equiv -X^4 \pmod{p}.$$

Therefore:

$$2X^4 \equiv 0 \pmod{p}, \quad 2Z^4 \equiv 0 \pmod{p}.$$

Hence $p \mid X$ and $p \mid Z$, which is a contradiction!
Conclusion: $\gcd(X^2 + Z^2, X^4 + Z^4)$ is a power of 2.
Therefore there is some W such that $cW^2 = X^4 + Z^4$, with $c \in \{1, 2\}$.
Dividing by Z^4, we obtain a rational point on the elliptic curve

$$E_c : cw^2 = (x^4 + 1).$$

We can do all this with `Magma`. First we find the set of twists to consider.

```
In [12]: Hk, AtoHk := TwoCoverDescent(X);
         deltas := { h@@AtoHk : h in Hk};
         deltas;
         g := x^4+1;
         L<Th> := quo<PolynomialRing(Rationals()) | g>;
         A := Domain(AtoHk);
         AtoL := hom<A->L|Th>;
         twist_list := {Norm(AtoL(delta)) : delta in deltas};
         twist_list;
```

```
{
    1,
    theta^4 - theta^3 + theta^2 + 1,
    -theta^3 - theta^2,
    -1/2*theta^5 + 1/2*theta^4 + 1/2*theta + 1/2
}
{ 1, 2 }
```

We find the points for the first twist.

```
In [13]: ellH := HyperellipticCurve(g);
         p0 := Setseq(Points(ellH:Bound:=10))[1];
         ell, ellHtoell := EllipticCurve(ellH, p0);
         ellHtoP1:=map<ellH->P1|[ellH.1,ellH.3]>;
         elltoP1:=Inverse(ellHtoell)*ellHtoP1;
         u := Extend(elltoP1);
         rk := Rank(ell); print "Rank(E) =", rk;
         #TorsionSubgroup(ell);
         ellrat := Points(ell:Bound:=2);
         #ellrat eq #TorsionSubgroup(ell);
         {u(P): P in ellrat};

Rank(E) = 0
4
true
{ (1 : 0), (0 : 1) }
```

And now for the second twist.

```
In [14]: ellH := HyperellipticCurve(2*g);
         p0 := Setseq(Points(ellH:Bound:=10))[1];
         ell, ellHtoell := EllipticCurve(ellH, p0);
         ellHtoP1:=map<ellH->P1|[ellH.1,ellH.3]>;
         elltoP1:=Inverse(ellHtoell)*ellHtoP1;
         u := Extend(elltoP1);
         rk := Rank(ell); print "Rank(E) =", rk;
         #TorsionSubgroup(ell);
         ellrat := Points(ell:Bound:=2);
         #ellrat eq #TorsionSubgroup(ell);
         {u(P): P in ellrat};

Rank(E) = 0
4
true
{ (1 : 1), (-1 : 1) }
```

We conclude that the solutions to $y^2 = (x^2+1)(x^4+1)$ have x-coordinate in $\{0, 1, -1\}$. We obtain the points:

$$\{\infty, (0, \pm 1), (\pm 1, \pm 2)\}.$$

This approach works in a lot more generality.

`Magma` (using an algorithm of Bruin-Stoll) gives us a finite list $\Delta \subseteq A = \mathbb{Q}[X]/(f(x))$ and curves

$$\phi_\delta \colon C_\delta \to X, \quad \delta \in \Delta$$

such that

$$X(\mathbb{Q}) = \bigcup_{\delta \in \Delta} C_\delta(\mathbb{Q}).$$

The curves C_δ have much larger genus, so Chabauty has a chance of working (theoretically).

However, computationally it's very hard to work with such curves (precisely because they have very large genus!).

If we factor $f(x) = g(x)h(x)$ over a number field K in such a way that $\deg g$ or $\deg h$ is even, then there is $d = d(\delta)$ and an unramified map $\psi_\delta \colon C_\delta \to E_d$.

Therefore, it's enough to determine

$$\phi_\delta(C_\delta(\mathbb{Q})) \subseteq \{P \in E_d(K) \colon x(P) \in \mathbb{P}^1(\mathbb{Q})\}.$$

As it turns out, `Magma` has a function (also called `Chabauty`) that can compute this latter set. This is what is known as **Elliptic curve Chabauty**.

Basic Idea: Suppose that $[K \colon \mathbb{Q}] = 2$ and that $E(K) = \langle P_0 \rangle$ has rank 1.

Consider $\log \colon E^1(K_v) \xrightarrow{\cong} K_v$, with inverse exp.

We can construct a power series

$$nP_0 = \exp(n \log(P_0)) \in \mathcal{O}_v[[n]].$$

We get a power series $\theta(n) \in \mathcal{O}_v[[n]]$.

Expressing $\mathcal{O}_v = \mathbb{Z}_p \oplus \alpha\mathbb{Z}_p$, we get $\theta(n) = \theta_0(n) + \alpha\theta_1(n)$, with $\theta_i(n) \in \mathbb{Z}_p[[n]]$.

The condition $x(P) \in \mathbb{P}^1(\mathbb{Q})$ translates in the condition $\theta_1(n) = 0$. The number of solutions to this can be bounded (Strassman).

2 Enrique's Curve

```
In [15]: f := 4*x^6 - 12*x^5 + 15*x^4 - 20*x^3 + 15*x^2 -  8*x + 4;
         X := HyperellipticCurve(f);
         X;
         Factorization(f);

Hyperelliptic Curve defined by y^2 = 4*x^6 - 12*x^5 + 15*x^4 - 20*x^3 + 15*x^2 -
    8*x + 4 over Rational Field
[
    <x - 2, 1>,
    <x^2 + 1, 1>,
    <x^3 - x^2 + 3/4*x - 1/2, 1>
]


In [16]: print "Points of X at infinity: ", PointsAtInfinity(X);
         Xrat := Points(X : Bound:=10000);
         print "Set of easily found rational points of X:", Xrat;
         uX := map<X -> P1 | [X.1, X.3]>;
         print "Set of x-coordinates: ", {uX(P) : P in Xrat};
```

```
Points of X at infinity:  {@ (1 : -2 : 0), (1 : 2 : 0) @}
Set of easily found rational points of X: {@ (1 : -2 : 0), (1 : 2 : 0), (0 : -2
: 1), (0 : 2 : 1), (2 : 0 : 1), (3 : -50 : 4), (3 : 50 : 4) @}
Set of x-coordinates:  { (2 : 1), (1 : 0), (0 : 1), (3/4 : 1) }
```

2.1 Goal: to prove that these are all the points of X

```
In [17]: Hk,AtoHk := TwoCoverDescent(X);
         A<theta> := Domain(AtoHk);
         AQ, AtoAQ := AbsoluteAlgebra(A);
         deltas := { h@@AtoHk : h in Hk};
         deltas;

{
    1,
    -228/25*theta^5 + 528/25*theta^4 - 499/25*theta^3 + 767/25*theta^2 -
        221/25*theta + 264/25,
    584/25*theta^5 - 1264/25*theta^4 + 1142/25*theta^3 - 2026/25*theta^2 +
        558/25*theta - 737/25,
    -34/5*theta^5 + 74/5*theta^4 - 119/10*theta^3 + 101/5*theta^2 - 51/10*theta
        + 32/5
}


In [18]: K<alpha> := AQ[3]; // We choose some field over which f factors more.
         K;
         AtoK := hom<A->K|alpha>;
         fac := Factorization(ChangeRing(f,K)); fac;
         g := fac[3][1] * fac[4][1]; // A choice of factorization of f

Number Field with defining polynomial x^3 + x^2 + 2*x - 2 over the Rational
Field
[
    <$.1 - 2, 1>,
    <$.1 + 1/2*(-alpha - 1), 1>,
    <$.1^2 + 1, 1>,
    <$.1^2 + 1/2*(alpha - 1)*$.1 + 1/4*(alpha^2 + 2), 1>
]


In [19]: L<Th> := quo<PolynomialRing(K) | g>;
         AtoL := hom<A->L|Th>;
         twist_list := Setseq({Norm(AtoL(delta)) : delta in deltas});
         twist_list;

[
    1,
    5*alpha^2 - 30*alpha + 20,
```

```
    4*alpha^2 - 4*alpha + 1,
    alpha^2 + alpha - 1
]
```

2.1.1 The `Chabauty` function

Input: 1. a map $\iota\colon A \twoheadrightarrow G \subset E(K)$ from an abstract group A into $E(K)$. 2. a map of varieties $u\colon E \to \mathbb{P}^1$ defined over K, and 3. a rational prime p, such that E and the map u have good reduction at primes above p.

Output: N, V, R, L, where: 1. $\#\{P \in G\colon u(P) \in \mathbb{P}^1(\mathbb{Q})\} \leq N$. 2. $V \subset A$ is some set of elements such that $u(\iota(v)) \in \mathbb{P}^1(\mathbb{Q})$ for all $v \in V$. 3. R is n integer such that if $\gcd([E(K)\colon G], R) = 1$ then

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

4. L is a collection of cosets in A such that together with V it contains all elements of A with rational image.

Upshot: if (3) is satisfied, **and** $\#V = N$ **and** L is empty, then

$$u(\{P \in E(K)\colon u(P) \in \mathbb{P}^1(\mathbb{Q})\}) = \{u(P)\colon P \in V\}.$$

```
In [20]: function test_points(u, p, aux: G := {1}, mwmap := 0)
             ell := Domain(u);
             print "Ed =", aInvariants(ell);
             if #G eq 1 then
                 success, G, mwmap := PseudoMordellWeilGroup(ell);
                 if not success then
                     G, mwmap := MordellWeilGroup(ell);
                     gs:=[mwmap(g): g in Generators(G)];
                     mwmap := map<G -> ell | a:->&+[a[i]*gs[i]:i in [1..#gs]] where a:=Eltseq(a
                 end if;
             end if;
             if IsFinite(G) then
                 print "Success! (Rank 0 Elliptic curve)";
                 return true, {u(mwmap(P)) : P in G | u(mwmap(P))[2] ne 0 and Degree(MinimalPol
             end if;
             N,V,R,L:=Chabauty(mwmap,u,p:Aux:= aux);
             print "supp(R) =", PrimeDivisors(R);
             N_is_upper_bound := &and[IsPSaturated(mwmap,p) : p in PrimeDivisors(R)];
             print "N is upper bound:", N_is_upper_bound;
             print "N =", N;
             print "V =", V;
             print "R =", R;
             print "L =", L;
             if N_is_upper_bound and (N eq #V) and (#L[2] eq 0) then
                 print "Success!";
                 return true, {EvaluateByPowerSeries(u,mwmap(P)):P in V};
             else
                 print "Fail!";
```

```
            return false, {EvaluateByPowerSeries(u,mwmap(P)):P in V};
        end if;
    end function;
```

```
In [21]: tw := 1; //twist_list[1];
         ellH := HyperellipticCurve(tw * g);
         p0 := Setseq( &join{Points(ellH,uX(P)[1]/uX(P)[2]) : P in Xrat | uX(P)[2] ne 0})[1];
         ell, ellHtoell := EllipticCurve(ellH, p0);
         ellHtoP1:=map<ellH->P1|[ellH.1,ellH.3]>;
         elltoP1:=Inverse(ellHtoell)*ellHtoP1;
         u := Extend(elltoP1);
         //test_points(u, 7, {});
         test_points(u, 43,{7,11,13,19,23,29,31});
```

```
Ed = [
    1/50*(-90*alpha^2 - 135*alpha + 213),
    1/5000*(-21735*alpha^2 - 47790*alpha + 33489),
    1/500000*(-12327390*alpha^2 - 22318335*alpha + 19743507),
    1/100000000*(-1527324255*alpha^2 - 5466100320*alpha + 4201955271),
    0
]
supp(R) = [ 2, 3 ]
N is upper bound: true
N = 4
V = {
    0,
    -2*G.2 - 3*G.3,
    G.1 - G.2 - G.3,
    G.1 - G.2 - 2*G.3
}
R = 24
L = <Mapping from: GrpAb: G to Abelian Group isomorphic to Z/2 + Z/24 + Z/168
Defined on 3 generators
Relations:
    2*$.1 = 0
    24*$.2 = 0
    168*$.3 = 0, {}>
Success!
true { (3/4 : 1), (1 : 0) }
```

```
In [22]: tw := 3*alpha^2 + 5*alpha + 9; //twist_list[2];
         ellH := HyperellipticCurve(tw * g);
         p0 := Setseq( &join{Points(ellH,uX(P)[1]/uX(P)[2]) : P in Xrat | uX(P)[2] ne 0})[1];
         ell, ellHtoell := EllipticCurve(ellH, p0);
         ellHtoP1:=map<ellH->P1|[ellH.1,ellH.3]>;
         elltoP1:=Inverse(ellHtoell)*ellHtoP1;
```

```
        u := Extend(elltoP1);
        test_points(u, 3,{});

Ed = [
    1/2*(alpha^2 - 1),
    1/8*(-3*alpha^2 - 12*alpha - 33),
    1/32*(17*alpha^2 + 24*alpha - 17),
    1/256*(261*alpha^2 - 340*alpha + 191),
    0
]
supp(R) = [ 2 ]
N is upper bound: true
N = 2
V = {
    0,
    G.1 - G.2
}
R = 2
L = <Mapping from: GrpAb: G to Abelian Group isomorphic to Z/12
Defined on 1 generator in supergroup:
    $.1 = 2*$.1
Relations:
    12*$.1 = 0, {}>
Success!
true { (0 : 1) }


In [23]: tw := -5*alpha^2 + 5*alpha + 5; //twist_list[3];
         ellH := HyperellipticCurve(tw * g);
         p0 := Points(ellH : Bound:=10)[1]; //Setseq( &join{Points(ellH,uX(P)[1]/uX(P)[2]) : P
         ell, ellHtoell := EllipticCurve(ellH, p0);
         ellHtoP1:=map<ellH->P1|[ellH.1,ellH.3]>;
         elltoP1:=Inverse(ellHtoell)*ellHtoP1;
         u := Extend(elltoP1);
         test_points(u, 3,{17,13,19,41,43,101});

Ed = [
    1/5*(alpha^2 + 4*alpha + 3),
    1/50*(-43*alpha^2 - 52*alpha - 81),
    1/500*(329*alpha^2 + 436*alpha - 445),
    1/10000*(-9451*alpha^2 + 6876*alpha - 993),
    0
]
supp(R) = [ 2 ]
N is upper bound: true
N = 2
V = {
    0,
```

```
    G.1 - 2*G.2
}
R = 16
L = <Mapping from: GrpAb: G to Abelian Group isomorphic to Z/16
Defined on 1 generator in supergroup:
    $.1 = 2*$.1
Relations:
    16*$.1 = 0, {}>
Success!
true { (2 : 1) }
```

```
In [24]: tw := 4*alpha^2 + 6*alpha + 11; //twist_list[4];
         ellH := HyperellipticCurve(tw * g);
         p0 := Points(ellH:Bound:=10)[1]; //Setseq( &join{Points(ellH,uX(P)[1]/uX(P)[2]) : P in
         ell, ellHtoell := EllipticCurve(ellH, p0);
         ellHtoP1:=map<ellH->P1|[ellH.1,ellH.3]>;
         elltoP1:=Inverse(ellHtoell)*ellHtoP1;
         u := Extend(elltoP1);
         test_points(u, 3,{});
```

```
Ed = [
    1/2*(alpha - 1),
    1/8*(-3*alpha^2 - 2*alpha - 23),
    1/32*(4*alpha^2 + 17*alpha - 15),
    1/256*(-135*alpha^2 + 104*alpha + 23),
    0
]
supp(R) = [ 2 ]
N is upper bound: true
N = 4
V = {
    0,
    G.1 - G.2,
    G.2 + G.3,
    G.1 + G.3
}
R = 2
L = <Mapping from: GrpAb: G to Abelian Group isomorphic to Z/12
Defined on 1 generator in supergroup:
    $.1 = 2*$.1
Relations:
    12*$.1 = 0, {}>
Success!
true { (3/4 : 1), (1 : 0) }
```

3 Thank you!