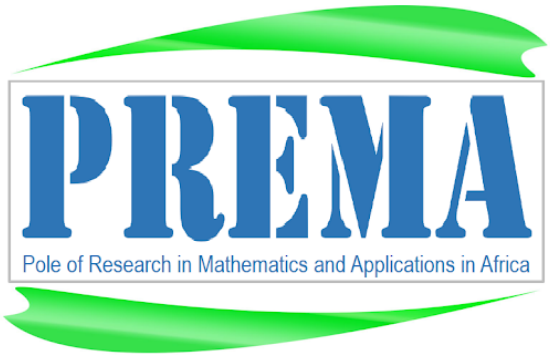
Rational points of some genus 3 curves from the rank 0 quotient strategy

Presented by MIAYOKA Brice

Marien Ngouabi university, Brazzaville-Congo



March 12, 2024

Outline

Given a projective, smooth, absolutely integral curve C over $\mathbb{Q}$, we are interested in determining the set $C(\mathbb{Q})$ of rational points on C. The genus g of C, which is a nonnegative integer depending on C up to birational equivalence, is an important data. If $g = 0$, then either $C(\mathbb{Q}) = \emptyset$ or C is isomorphic to the projective line. If $g = 1$ and $C(\mathbb{Q}) \neq \emptyset$, then C is an elliptic curve. In the latter case, a famous theorem by Mordell in [2] certifies that $C(\mathbb{Q})$ is a finitely generated abelian group.This means that $C(\mathbb{Q})$ can be described only from a finite number of its points. Moreover, at the end of his paper Mordell conjectured that if g is greater than or equal to 2, then $C(\mathbb{Q})$ is finite. In 1929, Weil [3] generalized the Mordell's theorem to all abelian varieties over number fields. And then, Faltings [4] proved the Mordell's conjecture in 1983. But Falting's proof is not effective. Actually, the problem of constructing an algorithm which computes the rational points of a given curve with genus ≥ 2 is of topical interest. There are some methods adapted to special families of curves, but the problem is difficult in general.

Genus 3 curves

Curves of genus 3 may be non-hyperelliptic (plane quartics) or hyperelliptic. we consider families of smooth curves of genus 3 given:

$$C1 : y^2 = f(x^2) = x^8 + ax^6 + bx^2 + cx^2 + d$$

where f is a polynomial irreducible of degree 4 de $\mathbf{Q}[x]$. $C1$, as defined is a hyperelliptic curve of genus 3 given by a model of even degree.
And the non-hyperelliptic curves given by the equation

$$C2 : ay^4 + (bx + c)y^3 + (dx^2 + ex + f)y^2 + (gx^3 + hx^2 + i)y +$$
$$jx^4 + kx^3 + lx^2 + mx + p = 0.$$

All coefficients are in $\mathbf{Q}$ and at least one of a, d, g, j is different from 0.
$C2$ is a plane quartic.

Chabauty-Coleman Method

One of the main known methods is based on the work by Chabauty and Coleman. Let C be a smooth projective curve of gene $g \geq 2$. Let J be its Jacobian. The Mordell-Weil theorem states that

$$J(\mathbb{Q}) = \mathbb{Z}^r \times J(\mathbb{Q})_{tors},$$

where $J(\mathbb{Q})_{tors}$ is the torsion subgroup of $J(\mathbb{Q})$ and $r \in \mathbb{N}$ is the rank of $J(\mathbb{Q})$ over $\mathbb{Q}$. Chabauty proved the following result:

Theorem

Let C be a smooth projective curve of gene $g \geq 2$. assume $C(\mathbb{Q}) \neq \emptyset$, then

$$C(\mathbb{Q}) \textit{ est fini}.$$

Chabauty-coleman

Let p be a prime of good reduction and Q_p. Let P$\in C(\mathbb{Q})$. *Then*

$$\begin{array}{rccc} \iota_P : & C & \longmapsto & J \\ & Q & \longmapsto & \overline{(Q-P)} \end{array}$$

Coleman made Chabauty's result effective by proving that we can have two things:

1. A finite subset of $C(\mathbb{Q}_p)$ which contains all rational points on C.

$$C(\mathbb{Q}_p)_1 = \{Q \in C(\mathbb{Q}_p) : \lambda_{\omega,D}(Q) = 0 \text{ for all } \omega \in Ann(J(\mathbb{Q})\}$$

where D a $\mathbb{Q}$-rational divisor on C of degree r, and
$Ann(J(\mathbb{Q})) =$
$$\left\{\omega_J \in \Omega_J(\mathbb{Q}_p) : \ \lambda_{\omega_J(R)} = \int_0^R \omega_J = 0 \text{ pour tout } R \in J(\mathbb{Q})\right\}$$

Chabauty-coleman

1. A bound on the set of rational points

$$\sharp C(\mathbb{Q}) \leq \sharp C(\mathbb{F}_p) + 2g - 2$$

If $r < g - 1$ and $p \geq 2g$, Stoll in [5], Corollary6.7], proves that

$$\sharp C(\mathbb{Q}) \leq \sharp C(\mathbb{F}_p) + 2r$$

Remark

Although this method is effective, we cannot apply it to these two families of curves $C1$, and $C2$. Coleman's method is conditioned by knowledge of the rank r. But there is no algorithm to calculate the rank of the Jacobian in the quartic plane case. And even in the case of hyperelliptic curves where we can calculate this rank, the algorithm does not return the rank directly but the limits.

Method quotient

Theorem

Let C be a smooth projective curve of genus $g \geq 2$. Then $Aut(C)$ is finite and

$$\#Aut(C) \leq 84(g-1)$$

$Aut(C)$ acts on C.
If C admits a non-trivial automorphism σ, then $G :=< \sigma >$ is a subgroup of $Aut(C)$. The set C/G is the set of orbits of G. In other words, it is the set of equivalence classes for the equivalence relation $\sim$ defined by $x \sim y$ if $y = gx$ for some $g \in G$.

$$Y := C/G \text{ is an algebraic curve.}$$

of genus $g' < g$.

Method quotient

Proposition The quotient C/G is smooth. The quotient map $q : C \longrightarrow Y := C/G$ is finite of degree $|G| := 2$. q is a non-constant curve morphism.

Theorem

$q(C(\mathbb{Q})) \subseteq Y(\mathbb{Q})$, *If we know* $Y(\mathbb{Q})$ *and it is finite, we can compute* $C(\mathbb{Q})$.

Elliptic curve

A curve E of genus 1 admitting at least one rational point is an elliptic curve, it is defined on $\mathbb{Q}$ by the equation

$$E : y^2 = x^3 + ax + b$$

where $a, b \in \mathbb{Q}$.

Theorem

(Mordell)

$$E(\mathbb{Q}) = \mathbb{Z}^r \times E(\mathbb{Q})_{tors},$$

where $E(\mathbb{Q})_{tors}$ *is the torsion subgroup of* $E(\mathbb{Q})$ *and* $r \in \mathbb{N}$ *is the rank of* $E(\mathbb{Q})$ *over* $\mathbb{Q}$.

If $r := 0$, then

$$E(\mathbb{Q}) := E(\mathbb{Q})_{tors}$$

it is finite group.

Mazur's theorem

Mazur [1], proved that this group is isomorphic to one of the following fifteen groups:

$$\mathbb{Z}/n\mathbb{Z}$$

with $1 \leq n \leq 10$ or $n = 12$,
and

$$\mathbb{Z}/2\mathbb{Z}x\mathbb{Z}/n\mathbb{Z}$$

with $1 \leq n \leq 4$.

Our Algorithm

We now specialize to two our cases of interest,

1rst case: C is an hyperelliptic curve is a genus 3 hyperelliptic curve given by an even degree model

$$y^2 := f(x^2)$$

where $f \in \mathbb{Q}[x]$, is of degree 8. C in this case admits an involution $\sigma_1 : (x, y) \to (-x, y)$, whose quotient E is an elliptic curve definied by the equation

$$E : y^2 := f(x)$$

Our Algorithm

2cd case: C is a genus 3 non-hyperelliptic curve(quartic plane) admitting at least one of the following involutions $\sigma_1 : (x, y) \to (-x, y)$, $\sigma_2 : (x, y) \to (x, -y)$, and $\sigma_3 : [x, y, z] \to [x, y, -z]$ (*projective model*), such that the quotient is genus 1 curve. If C does not admit one of the above involutions, then we can find the associated ternary form suppose that

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

Let m be a matrix nonsingular with coefficients in $\mathbb{Q}$

$$m = \begin{pmatrix} a_1 & b_3 & b_2 \\ b_3 & a_2 & b_1 \\ b_2 & b_1 & a_3 \end{pmatrix}$$

The curve

$$C_m : F(mX) = 0$$

is isomorphic at C.

Our Algorithm

Proposition Any plane quartic admitting at least two involutions which commute is geometrically isomorphic to a Ciani quartic.
we describe the algorithm we implemented to compute $C(\mathbb{Q})$for each C curve as defined above in our database. These curves come from Sutherland's database of genus 3 curves.
We began by filtering the database for those curves whose the quotient is genus 1 and have Mordell–Weil rank 0. We ran the Magma function **RankBounds(Jacobian(E))**.
If **RankBounds** returns 0 that prove E is rank 0, we proceed. Otherwise, we discard the curve and move on to the next one.

Our Algorithm

It turns out $38,564$ quartics plane have a rank 0 quotient curve, among them there are $17,404$ Ciani quartics. and 130 hyperelliptic curve have a genus 1 rank 0 quotient curve.
The algorithm can be summarized as follows

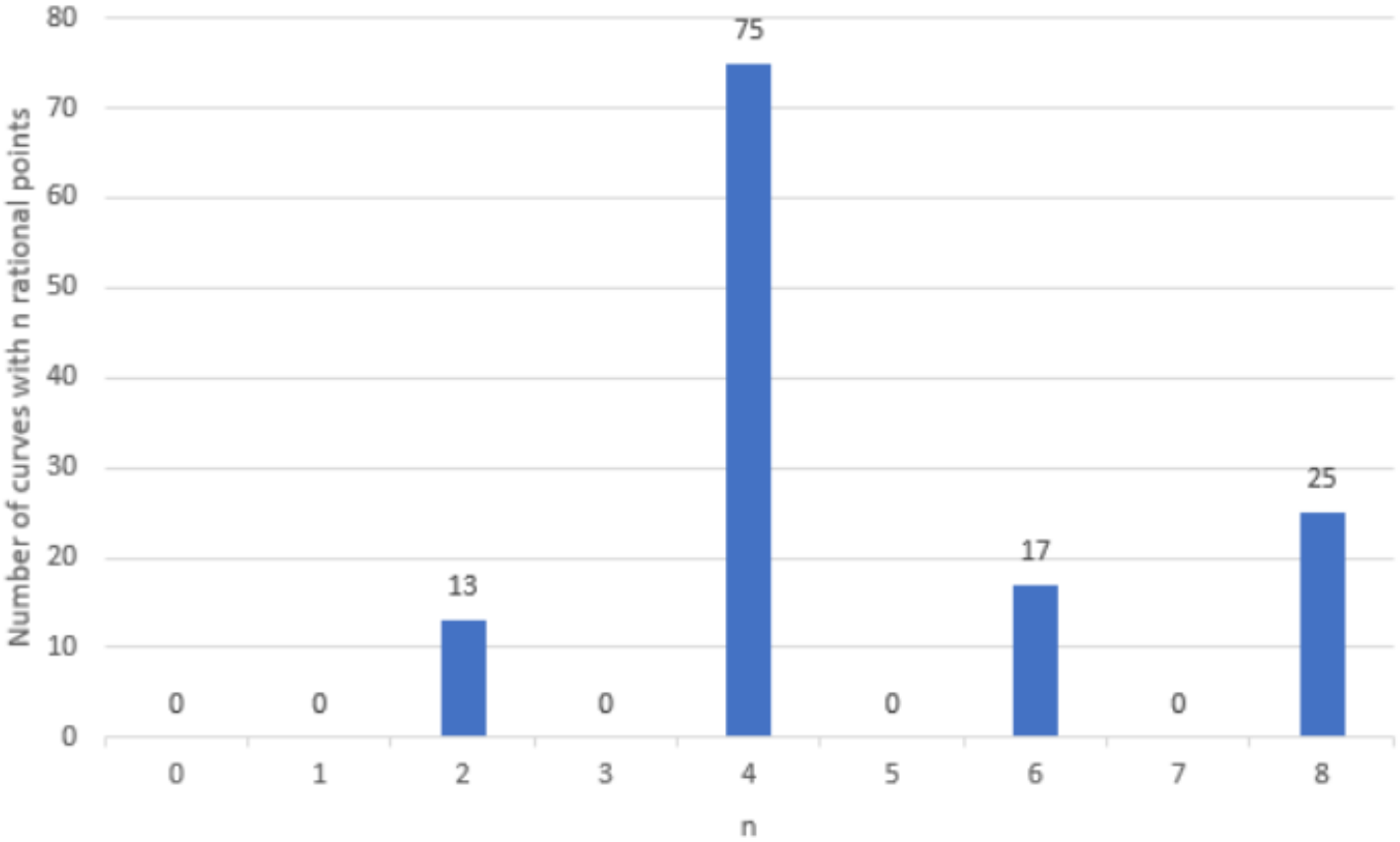
First case

Algorithm 1: Stratégie quotient de rang 0 sur les courbe hyperelliptiques de genre 3

Input: une courbe hyperelliptique d'équation $y^2 = x^8 + a_3x^6 + ... + a_1x^2 + 1$
Output: L'ensemble S des $\mathbb{Q}$ points de C

1 Calcule les deux courbes quotients C_i such that $\phi_i : C \to C_i$ $i = 1, 2$
2 Calcule le rang des jacobienne de C_1 .
3 Si $rank(C_1) = 0$ On calcule les points rationnels de C_1 qui sont les points de torsion.
4 Pour $i \in [1..\sharp C_1]$, nous calculons $\phi_1^{-1}(P_i)$ avec $P_i \in C_1(\mathbb{Q})$.
5 Détermine $S \subseteq \phi_1^{-1}(C_1(\mathbb{Q}))$
6 **return** S;

Graph


Number of curves with n rational points
80
70
60
50
40
30
20
10
0
0
0
13
0
75
0
17
0
25
0
1
2
3
4
5
6
7
8
n

Second case

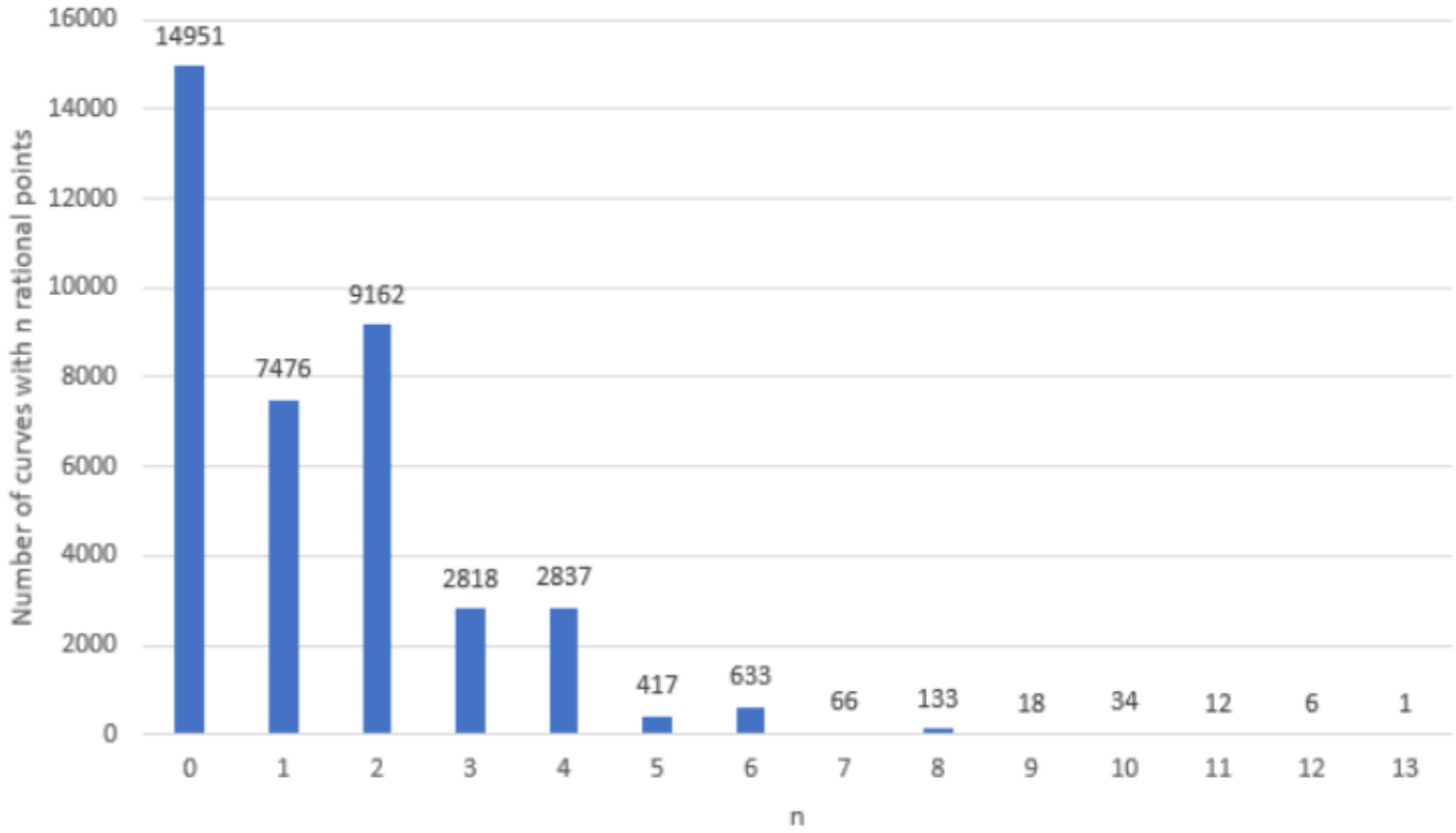
Algorithm 2: Stratégie quotient de rang 0 sur les quartiques planes

Input: Une quartique plane $C/\mathbb{Q}$ d'équation $F(x, y, z) = 0$ et $\chi := [[-x, y, z], [x, -y, z], [x, y, -z]]$

Output: L'ensemble S des $\mathbb{Q}$ points de C

1 Pour s dans χ calculer $F(s)$.
2 Si $F(s) := F(x, y, z)$ alors $\sigma : C \to C, s \to s$
3 Calculer $E := C/ < \sigma >$
4 Sinon Trouver une Matrice $m \in M_3(\mathbb{Q})$ non singulière
5 Trouver l'équation de C' : $H := F(m.X)$
6 Si $H(s) := H$, alors $\sigma : C \to C, s \to s$
7 Calculer $E := C'/ < \sigma >$, fin si;
8 Si rank(E):=0 alors calculer $E(\mathbb{Q})$
9 Si $E(\mathbb{Q}) = \varnothing$ alors $S = \varnothing$
10 Sinon calculer $\psi^{-1}(P)$ pour tout $P \in E(\mathbb{Q})$ Soit $\Omega(P) = \psi^{-1}(P) \bigcap D(\mathbb{Q})$ alors $S = \bigcup_{P \in D(\mathbb{Q})} \Omega(P)$ fin si;
11 **return** S;

Graph


Number of curves with n rational points
16000
14000
12000
10000
8000
6000
4000
2000
0
14951
7476
9162
2818
2837
417
633
66
133
18
34
12
6
1
0
1
2
3
4
5
6
7
8
9
10
11
12
13
n

Example1

The hyperelliptic curve

$$C : y^2z^6 = x^8 + 2x^4z^4 - 4x^2z^6 + z^8$$

is invariant under the symmetry

$$\alpha : C \longrightarrow C, [-x, y, z] \mapsto [-x, y, z]$$

, and the quotient

$$E := C/ < \alpha >$$

is a genus 1 rank 0 curve. By running our code, we found

$$E(\mathbb{Q}) = \{(0 : 1 : 0), (0 : 1/2 : 1), (0 : -1/2 : 1), (1 : 1/2 : 1), (1 : -1/2 : 1)\}$$

and $C(\mathbb{Q}) =$
$\{(1 : -1 : 0), (1 : 1 : 0), (-1 : 0 : 1), (0 : -1 : 1), (0 : 1 : 1), (1 : 0 : 1)\}$

Example

Consider the quartic plane $H := x^3y + x^2y^2 - 4xy^3 + 2y^4 + x^3z + 3x^2yz - 3xy^2z + x^2z^2 - 3xyz^2 + 3y^2z^2 - 4xz^3 + 2z^4 = 0$.

$$m := \begin{bmatrix} -2 & 0 & 0 \\ -1 & -2 & -2 \\ -1 & -2 & 2 \end{bmatrix}$$

$$Q(x, y, z) := H(AX) = H(-2x, -x - 2y - 2z, -x - 2y + 2z)$$

$$C : F(X^2, Y^2, Z^2) := 15X^4 - 88X^2Y^2 + 112Y^4 - 88X^2Z^2 + 288Y^2Z^2 + 112Z^4 = 0$$

Calculation of the curves E_i such that $phi_i : C \to E_i$ with $i = 1, 2, 3$.

Quotient by

$$\varphi_1(X,Y,Z) = (-X,Y,Z), \quad \varphi_2(X,Y,Z) = (X,-Y,Z), \quad \varphi_3(X,Y,Z) = (X,Y,-Z).$$

We obtain the quotient curves E_i of genus 1 on $\mathbb{Q}$ given by the equations

$$E_1 : F_1 := 112x^4 + 112y^4 + 15y^2z^2 - 88zy^3 - 88yzx^2 + 288x^2y^2 = 0$$
$$E_2 : F_2 := 112y^4 + 112z^4 + 15x^2z^2 - 88xz^3 - 88xzy^2 + 288z^2y^2 = 0$$
$$E_3 : F_3 := 112x^4 + 112z^4 + 15y^2x^2 - 88yx^3 - 88yxz^2 + 288x^2z^2 = 0$$

We find that these three curves E_i admit the following Weierstrass model

$$E : y^2 = x^3 + \frac{7}{2}x^2 - \frac{15}{16}x$$

avec les transformations suivantes: $E_1 \longrightarrow E : (x,y,z) \mapsto$
$(28/15x^2y + 58/15y^3 - y^2z, 56/15x^3 + 116/15xy^2 - 2xyz, -8/15y^3)$
$E_2 \longrightarrow E : (x,y,z) \mapsto$
$(28/15y^2z + 58/15z^3 - z^2x, 56/15y^3 + 116/15yz^2 - 2xyz, -8/15z^3)$
$E_3 \longrightarrow E : (x,y,z) \mapsto$
$(28/15z^2x + 58/15x^3 - x^2y, 56/15z^3 + 116/15zx^2 - 2xyz, -8/15x^3)$

Using Magma, the Mordell rank of E is 0, so $E(\mathbb{Q})$ is finite.

$$E(\mathbb{Q}) = \{\infty, (0,0), (-3/4, -3/2), (-3/4, 3/2), (1/4, 0),$$
$$(5/4, -5/2), (5/4, 5/2), (-15/4, 0)$$

en calculant $\phi_i^{-1}(E(\mathbb{Q}))$, notre code retourne que

$$C(\mathbb{Q}) = \{(2:1:0), (2:0:1), (-2:1:0), (-2:0:1)\}$$

We have noticed that this curve is precise in $p = 17$, $C(\mathbb{F}_{17}) = \{(2:0:1), (15:0:1), (2:1:0), (15:1:0)\}$, We then use $\sharp C(\mathbb{Q}) \leq \sharp C(\mathbb{F}_{17}) + 2r$, C is sharp.

https://github.com/Brice202145/Strategie$_R$ang$_q$uotient

Bibliography

- B. Mazur. Modular curves and the Eisenstein ideal. Publ. Math., Inst. Hautes Étud. Sci., 47:33–186, 1977
- L. J. Mordell. On the rational solutions of the indeterminate equations of the third and fourth degrees. Proc. Camb. Philos. Soc., 21:179–192, 1922.
- A. Sutherland. A database of nonhyperelliptic genus 3 curves over q. Available at

  https://math.mit.edu/ drew/gce$_g$*enus*3$_n$*onhyperelliptic*.*txtG*.*Faltings*.*En* 349–366, 1983.*Anoptionalnote*.

- A. Weil. L'arithmétique sur les courbes algébriques. Acta Math., 52:281315, 1929.
- Michael Stoll. Independence of rational points on twists of a given curve. Compos. Math., 142(5):1201–1214, 2006.

The End

THANK YOU