Properties of elliptic curves with a point of order n over number fields of degree d

Filip Najman

University of Zagreb

Arithmetic Aspects of Explicit Moduli Problems
Banff, May 29th 2017.

Subject of this talk

Let E/K be an elliptic curve, where K is a number field of degree d, such that $E(K)$ contains a point of order n.

Subject of this talk

Let E/K be an elliptic curve, where K is a number field of degree d, such that $E(K)$ contains a point of order n.

What properties do E and K have?

Subject of this talk

Let E/K be an elliptic curve, where K is a number field of degree d, such that $E(K)$ contains a point of order n.

What properties do E and K have?

What can we say about the field K itself, about the rank of E over K (or over extensions of K), the reduction types of E at primes of K, the field of definition of E and $j(E)$, etc.?

It is reasonable to start with $d = 1$, i.e. to look at elliptic curves over $\mathbb{Q}$.

Elliptic curves with a point of order n over $\mathbb{Q}$

It is reasonable to start with $d = 1$, i.e. to look at elliptic curves over $\mathbb{Q}$.

Mazur (1977): The torsion of an elliptic curve over $\mathbb{Q}$ is isomorphic to one of the following groups:

$$C_n, \text{ where } n = 1, \dots, 10 \text{ or } 12,$$

$$C_2 \oplus C_{2n}, \text{ where } n = 1, \dots, 4.$$

Elliptic curves with a point of order n over $\mathbb{Q}$

It is reasonable to start with $d = 1$, i.e. to look at elliptic curves over $\mathbb{Q}$.

Mazur (1977): The torsion of an elliptic curve over $\mathbb{Q}$ is isomorphic to one of the following groups:

$$C_n, \text{ where } n = 1, \dots, 10 \text{ or } 12,$$

$$C_2 \oplus C_{2n}, \text{ where } n = 1, \dots, 4.$$

Unfortunately, one cannot say much about an elliptic curve with a point of order n over $\mathbb{Q}$.

Elliptic curves with a point of order n over $\mathbb{Q}$

It is reasonable to start with $d = 1$, i.e. to look at elliptic curves over $\mathbb{Q}$.

Mazur (1977): The torsion of an elliptic curve over $\mathbb{Q}$ is isomorphic to one of the following groups:

$$C_n, \text{ where } n = 1, \dots, 10 \text{ or } 12,$$

$$C_2 \oplus C_{2n}, \text{ where } n = 1, \dots, 4.$$

Unfortunately, one cannot say much about an elliptic curve with a point of order n over $\mathbb{Q}$.

The reason is that all the curves $X_1(n)$ with non-cuspidal points over $\mathbb{Q}$ (i.e. $n \leq 10$ or $n = 12$), are of genus 0.

Let E/K be an elliptic curve, where K is a number field of degree d, with a point of order n.

1) For $(n, d) = (13, 2)$:
   a) K is a real quadratic field.

Elliptic curves with a point of order n over quadratic fields

Let E/K be an elliptic curve, where K is a number field of degree d, with a point of order n.

1) For $(n, d) = (13, 2)$:
   a) K is a real quadratic field.
   b) E is isomorphic to its Galois conjugate E^σ and $j(E) \in \mathbb{Q}$ (but E itself is not defined over $\mathbb{Q}$!). So E is a $\mathbb{Q}$-curve.

Let E/K be an elliptic curve, where K is a number field of degree d, with a point of order n.

1) For $(n, d) = (13, 2)$:
   a) K is a real quadratic field.
   b) E is isomorphic to its Galois conjugate E^σ and $j(E) \in \mathbb{Q}$ (but E itself is not defined over $\mathbb{Q}$!). So E is a $\mathbb{Q}$-curve.
   c) E has even rank over K.

Elliptic curves with a point of order n over quadratic fields

Let E/K be an elliptic curve, where K is a number field of degree d, with a point of order n.

1) For $(n, d) = (13, 2)$:
   a) K is a real quadratic field.
   b) E is isomorphic to its Galois conjugate E^σ and $j(E) \in \mathbb{Q}$ (but E itself is not defined over $\mathbb{Q}$!). So E is a $\mathbb{Q}$-curve.
   c) E has even rank over K.
   d) E has even rank over every number field N that can be written as $N = N' \otimes_{\mathbb{Q}} K$ for some number field N'.

Let E/K be an elliptic curve, where K is a number field of degree d, with a point of order n.

1) For $(n, d) = (13, 2)$:
   a) K is a real quadratic field.
   b) E is isomorphic to its Galois conjugate E^σ and $j(E) \in \mathbb{Q}$ (but E itself is not defined over $\mathbb{Q}$!). So E is a $\mathbb{Q}$-curve.
   c) E has even rank over K.
   d) E has even rank over every number field N that can be written as $N = N' \otimes_{\mathbb{Q}} K$ for some number field N'.
   e) The product $\prod_v c_v$ of the Tamagawa numbers c_v of E satisfies that $v_{13}(\prod_v c_v)$ is a positive even integer and there exists exactly one elliptic curve for which $v_{13}(\prod_v c_v) = 2$.

Elliptic curves with a point of order n over quadratic fields

Let E/K be an elliptic curve, where K is a number field of degree d, with a point of order n.

1) For $(n, d) = (13, 2)$:
   a) K is a real quadratic field.
   b) E is isomorphic to its Galois conjugate E^σ and $j(E) \in \mathbb{Q}$ (but E itself is not defined over $\mathbb{Q}$!). So E is a $\mathbb{Q}$-curve.
   c) E has even rank over K.
   d) E has even rank over every number field N that can be written as $N = N' \otimes_{\mathbb{Q}} K$ for some number field N'.
   e) The product $\prod_v c_v$ of the Tamagawa numbers c_v of E satisfies that $v_{13}(\prod_v c_v)$ is a positive even integer and there exists exactly one elliptic curve for which $v_{13}(\prod_v c_v) = 2$.

a), b) and c) were proved by Bosman, Bruin, Dujella and N. (2011), a) was independently also proven by Krumm (2012), d) by Bruin and N. (2012), and e) by N. (2016)

2) For $(n, d) = (16, 2)$, E is defined over $\mathbb{Q}$, i.e. E/K is a base change of an elliptic curve defined over $\mathbb{Q}$. Moreover $E(\mathbb{Q})_{tors} \simeq C_8$ and E has a $\mathbb{Q}$-rational 16-isogeny.

2) For $(n, d) = (16, 2)$, E is defined over $\mathbb{Q}$, i.e. E/K is a base change of an elliptic curve defined over $\mathbb{Q}$. Moreover $E(\mathbb{Q})_{tors} \simeq C_8$ and E has a $\mathbb{Q}$-rational 16-isogeny.
3) For $(n, d) = (18, 2)$,
    a) K is a real quadratic field.

2) For $(n, d) = (16, 2)$, E is defined over $\mathbb{Q}$, i.e. E/K is a base change of an elliptic curve defined over $\mathbb{Q}$. Moreover $E(\mathbb{Q})_{tors} \simeq C_8$ and E has a $\mathbb{Q}$-rational 16-isogeny.
3) For $(n, d) = (18, 2)$,
   a) K is a real quadratic field.
   b) E is 2-isogenous (over K) to its Galois conjugate E^σ, so E is a $\mathbb{Q}$-curve.

2) For $(n, d) = (16, 2)$, E is defined over $\mathbb{Q}$, i.e. E/K is a base change of an elliptic curve defined over $\mathbb{Q}$. Moreover $E(\mathbb{Q})_{tors} \simeq C_8$ and E has a $\mathbb{Q}$-rational 16-isogeny.
3) For $(n, d) = (18, 2)$,
   a) K is a real quadratic field.
   b) E is 2-isogenous (over K) to its Galois conjugate E^σ, so E is a $\mathbb{Q}$-curve.
   c) E has even rank over K

2) For $(n, d) = (16, 2)$, E is defined over $\mathbb{Q}$, i.e. E/K is a base change of an elliptic curve defined over $\mathbb{Q}$. Moreover $E(\mathbb{Q})_{tors} \simeq C_8$ and E has a $\mathbb{Q}$-rational 16-isogeny.
3) For $(n, d) = (18, 2)$,
   a) K is a real quadratic field.
   b) E is 2-isogenous (over K) to its Galois conjugate E^σ, so E is a $\mathbb{Q}$-curve.
   c) E has even rank over K
   d) E has even rank over every number field N that can be written as $N = N' \otimes_{\mathbb{Q}} K$ for some number field N'.

2) For $(n, d) = (16, 2)$, E is defined over $\mathbb{Q}$, i.e. E/K is a base change of an elliptic curve defined over $\mathbb{Q}$. Moreover $E(\mathbb{Q})_{tors} \simeq C_8$ and E has a $\mathbb{Q}$-rational 16-isogeny.
3) For $(n, d) = (18, 2)$,
   a) K is a real quadratic field.
   b) E is 2-isogenous (over K) to its Galois conjugate E^{σ}, so E is a $\mathbb{Q}$-curve.
   c) E has even rank over K
   d) E has even rank over every number field N that can be written as $N = N' \otimes_{\mathbb{Q}} K$ for some number field N'.

2) was proved by Bruin and N. (2016), 3a), 3b), 3c) by BBDN (2011), and 3a) also independently by Krumm (2012) and 3d) by Bruin and N. (2012)

4) For $(n, d) = (21, 3)$, (E, K) is unique

$$E : y^2 + xy + y = x^3 - x^2 - 5x + 5,$$

and $K = \mathbb{Q}(\zeta_9)^+$.

5) If $E(K)_{tors}$ contains $C_2 \oplus C_{14}$ as a subgroup, then K is a cyclic cubic field and E is a base change of an elliptic curve over $\mathbb{Q}$.

The curve in 4) was found by N. (2012), and proven to be unique by Derickx, Etropolski, Morrow and Zuerick-Brown (?). Statement 5) was proved by Bruin and N. (2016)

6) For $(n, d) = (22, 4)$,
   a) The Galois group of the normal closure of K over $\mathbb{Q}$ is D_4.

6) For $(n, d) = (22, 4)$,
   a) The Galois group of the normal closure of K over $\mathbb{Q}$ is D_4.
   b) E is 2-isogenous to E^{σ}, where σ is the generator of $\mathrm{Gal}(K/L)$, and where L is the unique quadratic subfield of K. So E is a L-curve.

6) For $(n, d) = (22, 4)$,
   a) The Galois group of the normal closure of K over $\mathbb{Q}$ is D_4.
   b) E is 2-isogenous to E^σ, where σ is the generator of $\mathrm{Gal}(K/L)$, and where L is the unique quadratic subfield of K. So E is a L-curve.
   c) E has even rank over K

6) For $(n, d) = (22, 4)$,
   a) The Galois group of the normal closure of K over $\mathbb{Q}$ is D_4.
   b) E is 2-isogenous to E^σ, where σ is the generator of $\mathrm{Gal}(K/L)$, and where L is the unique quadratic subfield of K. So E is a L-curve.
   c) E has even rank over K
7) For $(n, d) = (17, 4)$, the Galois group of the normal closure of K over $\mathbb{Q}$ is D_4 or S_4, with finitely many exceptions.

6) was proven by BBDN (2011) and 7) by Derickx, Kamienny and Mazur (2015).

Moduli interpretation of maps between modular curves

All of these results come from finding all the maps from the corresponding modular curve $X := X_1(n)$ to all possible quotients X' of X of genus 0, and understanding the moduli interpretation of X' and the maps $X \to X'$.

Moduli interpretation of maps between modular curves

All of these results come from finding all the maps from the corresponding modular curve $X := X_1(n)$ to all possible quotients X' of X of genus 0, and understanding the moduli interpretation of X' and the maps $X \to X'$.

We will sketch the case when X is a hyperelliptic curve, i.e $X = X_1(n)$ for $n = 13, 16, 18$.

Moduli interpretation of maps between modular curves

All of these results come from finding all the maps from the corresponding modular curve $X := X_1(n)$ to all possible quotients X' of X of genus 0, and understanding the moduli interpretation of X' and the maps $X \to X'$.

We will sketch the case when X is a hyperelliptic curve, i.e $X = X_1(n)$ for $n = 13, 16, 18$.

All the other cases follow the same basic ideas, although they are more technically complicated.

Hyperelliptic modular curves

Let E/K be an elliptic curve with a point of order n over a quadratic field K such that $X := X_1(n)$ is hyperelliptic. Let J be the Jacobian of X, ι the (unique) hyperelliptic involution of X and σ the generator of $\mathrm{Gal}(K/\mathbb{Q})$.

Fix a cusp $C \in X(\mathbb{Q})$. We look at the map

$$f : \mathrm{Sym}^2 X \to J,$$

$$\{P, Q\} \to [P + Q - C - \iota(C)],$$

which is an isomorphism away from the fibre above 0 which consists of the pairs of points $\{P, \iota(P)\}$ which are fixed by ι.

Let E/K be an elliptic curve with a point of order n over a quadratic field K such that $X := X_1(n)$ is hyperelliptic. Let J be the Jacobian of X, ι the (unique) hyperelliptic involution of X and σ the generator of $\mathrm{Gal}(K/\mathbb{Q})$.

Fix a cusp $C \in X(\mathbb{Q})$. We look at the map

$$f : \mathrm{Sym}^2 X \to J,$$

$$\{P, Q\} \to [P + Q - C - \iota(C)],$$

which is an isomorphism away from the fibre above 0 which consists of the pairs of points $\{P, \iota(P)\}$ which are fixed by ι.

In all our cases we get that $J(\mathbb{Q})$ is finite and, we compute that $f^{-1}(J(\mathbb{Q}) - \{0\})$ consists only of pairs of cusps.

Hyperelliptic modular curves

Let E/K be an elliptic curve with a point of order n over a quadratic field K such that $X := X_1(n)$ is hyperelliptic. Let J be the Jacobian of X, ι the (unique) hyperelliptic involution of X and σ the generator of $\mathrm{Gal}(K/\mathbb{Q})$.

Fix a cusp $C \in X(\mathbb{Q})$. We look at the map

$$f : \mathrm{Sym}^2 X \to J,$$

$$\{P, Q\} \to [P + Q - C - \iota(C)],$$

which is an isomorphism away from the fibre above 0 which consists of the pairs of points $\{P, \iota(P)\}$ which are fixed by ι.

In all our cases we get that $J(\mathbb{Q})$ is finite and, we compute that $f^{-1}(J(\mathbb{Q}) - \{0\})$ consists only of pairs of cusps.

Now take a non-cusp point P in $X(K)$. Then $f(\{P, P^\sigma\}) \in J(\mathbb{Q})$, thus it has to be 0, so $P^\sigma = \iota(P)$.

Hyperelliptic modular curves

To conclude: the only non-cusp quadratic points on X are such that $\iota(P) = P^{\sigma}$.

Hyperelliptic modular curves

To conclude: the only non-cusp quadratic points on X are such that $\iota(P) = P^\sigma$.

Note that this is general fact about hyperelliptic curves: using the notation as above, for a hyperelliptic curve over a number field L, the points P of degree 2 over L are those such that $P^\sigma = \iota(P)$ together with those that lie in $f^{-1}(J(L) - \{0\})$.

Hyperelliptic modular curves

To conclude: the only non-cusp quadratic points on X are such that $\iota(P) = P^\sigma$.

Note that this is general fact about hyperelliptic curves: using the notation as above, for a hyperelliptic curve over a number field L, the points P of degree 2 over L are those such that $P^\sigma = \iota(P)$ together with those that lie in $f^{-1}(J(L) - \{0\})$.

Taking a model $X : y^2 = f(x)$, we have that all the quadratic non-cusp points are of the form $(x, \sqrt{f(x)})$, for some $x \in \mathbb{Q}$. Now it happens that for $X = X_1(13)$ and $X_1(18)$, for all $x \in \mathbb{R}$, $f(x)$ is positive. Hence there are no non-cuspidal points on these modular curves are defined over imaginary quadratic fields.

Hyperelliptic modular curves

Recall that each point $x \in X_1(n)$ represents a K-isomorphism class of (E, P), where E/K and $P \in E(K)$ has order n. Then x^σ represents (E^σ, P^σ). The moduli interpretation of ι is the following

1. For $n = 13$,$\iota((E, P)) = (E, 5P)$. Now since $\iota(x) = x^\sigma$ we have $E \simeq E^\sigma$.
2. For $n = 16$, $\iota((E, P)) = (E, 9P)$. Again, since $\iota(x) = x^\sigma$ we have $E \simeq E^\sigma$.
3. For $n = 18$, $\iota((E, P)) = (E/\langle 9P\rangle, Q)$, where Q is a point of order 18. We have that E is 2-isogenous to E^σ.

Understanding $E \simeq E^\sigma$

To get information about the field of definition of E, one has to understand the isomorphism $E \simeq E^\sigma$.

Understanding $E \simeq E^\sigma$

To get information about the field of definition of E, one has to understand the isomorphism $E \simeq E^\sigma$.

Take now $X = X_1(13)$ and let ϕ be the isomorphism from (E^σ, P^σ) to $(E, 5P)$ coming from $x^\sigma = \iota(x)$. Then

$$(\phi \circ \sigma)(E, P) = (E, 5P),$$

$$(\phi \circ \sigma)^2(E, P) = (E, 25P) = (E, -P).$$

Understanding $E \simeq E^\sigma$

To get information about the field of definition of E, one has to understand the isomorphism $E \simeq E^\sigma$.

Take now $X = X_1(13)$ and let ϕ be the isomorphism from (E^σ, P^σ) to $(E, 5P)$ coming from $x^\sigma = \iota(x)$. Then

$$(\phi \circ \sigma)(E, P) = (E, 5P),$$

$$(\phi \circ \sigma)^2(E, P) = (E, 25P) = (E, -P).$$

Now it is obvious that ϕ cannot be the identity, hence σ does not act trivially on E, and hence E is not defined over $\mathbb{Q}$.

Understanding $E \simeq E^\sigma$

To get information about the field of definition of E, one has to understand the isomorphism $E \simeq E^\sigma$.

Take now $X = X_1(13)$ and let ϕ be the isomorphism from (E^σ, P^σ) to $(E, 5P)$ coming from $x^\sigma = \iota(x)$. Then

$$(\phi \circ \sigma)(E, P) = (E, 5P),$$

$$(\phi \circ \sigma)^2(E, P) = (E, 25P) = (E, -P).$$

Now it is obvious that ϕ cannot be the identity, hence σ does not act trivially on E, and hence E is not defined over $\mathbb{Q}$.

Moreover $(\phi \circ \sigma) = \sqrt{-1}$ is an endomorphism of $E(K)$, which is not mulitplicaiton by n, hence $E(K)$ is a $\mathbb{Z}[i]$-module, and hence a $\mathbb{Z}$-module of even rank. Equivalently, $\mathrm{End}(\mathrm{Res}_{K/\mathbb{Q}} E) \simeq \mathbb{Z}[\sqrt{-1}]$.

Remaining cases

In the case $X_1(16)$ one can work out that $E^\sigma = E$, so E has a model defined over $\mathbb{Q}$. Moreover, for the point P of order 16, one gets that $2P = (2P)^\sigma$, so $E(\mathbb{Q})$ contains a point of order 8.

Remaining cases

In the case $X_1(16)$ one can work out that $E^\sigma = E$, so E has a model defined over $\mathbb{Q}$. Moreover, for the point P of order 16, one gets that $2P = (2P)^\sigma$, so $E(\mathbb{Q})$ contains a point of order 8.

In all the above cases we took advanatage of the moduli interpretation of the map $X \to X/\iota$. It was very convenient that there is a unique map from X to $\mathbb{P}^1$ for hyperelliptic X.

Remaining cases

In the case $X_1(16)$ one can work out that $E^\sigma = E$, so E has a model defined over $\mathbb{Q}$. Moreover, for the point P of order 16, one gets that $2P = (2P)^\sigma$, so $E(\mathbb{Q})$ contains a point of order 8.

In all the above cases we took advanatage of the moduli interpretation of the map $X \to X/\iota$. It was very convenient that there is a unique map from X to $\mathbb{P}^1$ for hyperelliptic X.

For X of higher gonality, there is usually more than one map from X to $\mathbb{P}^1$, so things become more complicated.

Tamagawa numbers

Let E/K an elliptic curve over a number field K. For every finite prime v of K, denote by K_v the completion of K at v and by k_v the residue field of v. The subgroup $E_0(K_v)$ of $E(K_v)$ consisting of points that reduce to nonsingular points in $E(k_v)$ has finite index in $E(K_v)$ and the *Tamagawa number* of E at v is this index $c_v := [E(K_v) : E_0(K_v)]$.

Let E/K an elliptic curve over a number field K. For every finite prime v of K, denote by K_v the completion of K at v and by k_v the residue field of v. The subgroup $E_0(K_v)$ of $E(K_v)$ consisting of points that reduce to nonsingular points in $E(k_v)$ has finite index in $E(K_v)$ and the *Tamagawa number* of E at v is this index $c_v := [E(K_v) : E_0(K_v)]$.

Define c_E to be $c_E := \prod_v c_v$.

Tamagawa numbers

Let E/K an elliptic curve over a number field K. For every finite prime v of K, denote by K_v the completion of K at v and by k_v the residue field of v. The subgroup $E_0(K_v)$ of $E(K_v)$ consisting of points that reduce to nonsingular points in $E(k_v)$ has finite index in $E(K_v)$ and the *Tamagawa number* of E at v is this index $c_v := [E(K_v) : E_0(K_v)]$.

Define c_E to be $c_E := \prod_v c_v$.

Because the ratio $c_E/\#E(K)_{tors}$ appears, by the Birch-Swinnerton–Dyer conjecture, as a factor in the leading term of the L-function of E, it is natural to study how the value of c_E depends on $E(K)_{tors}$.

Tamagawa numbers

Let E/K an elliptic curve over a number field K. For every finite prime v of K, denote by K_v the completion of K at v and by k_v the residue field of v. The subgroup $E_0(K_v)$ of $E(K_v)$ consisting of points that reduce to nonsingular points in $E(k_v)$ has finite index in $E(K_v)$ and the *Tamagawa number* of E at v is this index $c_v := [E(K_v) : E_0(K_v)]$.

Define c_E to be $c_E := \prod_v c_v$.

Because the ratio $c_E/\#E(K)_{tors}$ appears, by the Birch-Swinnerton–Dyer conjecture, as a factor in the leading term of the L-function of E, it is natural to study how the value of c_E depends on $E(K)_{tors}$.

Lorenzini (2011) proved many results about this ratio for elliptic curves over $\mathbb{Q}$.

The ratio $c_E/\#E(K)_{tors}$

Suppose for simplicity that $N = \#E(K)_{tors}$ is prime. Let $E_1(K_v)$ be the subgroup of $E(K_v)$ of points which reduce to the point at infinity in $E(k_v)$ and let $E_{ns}(k_v)$ be the group of nonsingular points in $E(k_v)$.

The ratio $c_E/\#E(K)_{tors}$

Suppose for simplicity that $N = \#E(K)_{tors}$ is prime. Let $E_1(K_v)$ be the subgroup of $E(K_v)$ of points which reduce to the point at infinity in $E(k_v)$ and let $E_{ns}(k_v)$ be the group of nonsingular points in $E(k_v)$.

There exists an exact sequence of abelian groups

$$0 \longrightarrow E_1(K_v) \longrightarrow E_0(K_v) \longrightarrow E_{ns}(k_v) \longrightarrow 0.$$

The ratio $c_E/\#E(K)_{tors}$

Suppose for simplicity that $N = \#E(K)_{tors}$ is prime. Let $E_1(K_v)$ be the subgroup of $E(K_v)$ of points which reduce to the point at infinity in $E(k_v)$ and let $E_{ns}(k_v)$ be the group of nonsingular points in $E(k_v)$.

There exists an exact sequence of abelian groups

$$0 \longrightarrow E_1(K_v) \longrightarrow E_0(K_v) \longrightarrow E_{ns}(k_v) \longrightarrow 0.$$

If v does not divide N, then there are no points of order N in $E_1(K_v)$, as $E_1(K_v)$ is isomorphic to the formal group of E. If v is also small enough such that there cannot be any points of order N in $E_{ns}(k_v)$, then it follows that $E_0(K_v)$ does not have a point of order N. It then follows, by definition, that N has to divide c_v.

The ratio $c_E/\#E(K)_{tors}$

Suppose for simplicity that $N = \#E(K)_{tors}$ is prime. Let $E_1(K_v)$ be the subgroup of $E(K_v)$ of points which reduce to the point at infinity in $E(k_v)$ and let $E_{ns}(k_v)$ be the group of nonsingular points in $E(k_v)$.

There exists an exact sequence of abelian groups

$$0 \longrightarrow E_1(K_v) \longrightarrow E_0(K_v) \longrightarrow E_{ns}(k_v) \longrightarrow 0.$$

If v does not divide N, then there are no points of order N in $E_1(K_v)$, as $E_1(K_v)$ is isomorphic to the formal group of E. If v is also small enough such that there cannot be any points of order N in $E_{ns}(k_v)$, then it follows that $E_0(K_v)$ does not have a point of order N. It then follows, by definition, that N has to divide c_v.

Krumm showed (taking v to be a prime above 2 and $N = 13$) that for all elliptic curves E over all quadratic fields K with $E(K)_{tors} \simeq C_{13}$, $v_{13}(c_E) \geq 2$.

A conjecture of Krumm

Krumm noticed that for the first 48925 such elliptic curves E that he tested it was always true that $v_{13}(c_E)$ is even. He conjectured that this was always the case.

A conjecture of Krumm

Krumm noticed that for the first 48925 such elliptic curves E that he tested it was always true that $v_{13}(c_E)$ is even. He conjectured that this was always the case.

Let for the remainder of the talk $X = X_1(13)$, and let J be the Jacobian of X. The cusps of X are defined over $\mathbb{Q}(\zeta_{13})^+$ and none of them are fixed by ι. The rank of $J(\mathbb{Q}(\zeta_{13})^+)$ is 0.

Krumm noticed that for the first 48925 such elliptic curves E that he tested it was always true that $v_{13}(c_E)$ is even. He conjectured that this was always the case.

Let for the remainder of the talk $X = X_1(13)$, and let J be the Jacobian of X. The cusps of X are defined over $\mathbb{Q}(\zeta_{13})^+$ and none of them are fixed by ι. The rank of $J(\mathbb{Q}(\zeta_{13})^+)$ is 0.

Lemma. Let $(E, P) = x \in X(K)$, let v be a prime of K such that $v \nmid 13$ and $13 | c_v$, let p be the rational prime below v and let v' be a prime of $\mathbb{Q}(\zeta_{13})^+$ above p. Then x mod v is equal to C mod v' for a cusp $C \in X(\mathbb{Q}(\zeta_{13})^+)$ such that C mod v' is $\mathbb{F}_p$-rational.

Proposition Let E_t be an elliptic curve over a quadratic field K with $E_t(K)_{tors} \simeq C_{13}$. Let v be a prime of K over a rational prime p such that 13 divides c_v. Then p splits in K.

Proposition Let E_t be an elliptic curve over a quadratic field K with $E_t(K)_{tors} \simeq C_{13}$. Let v be a prime of K over a rational prime p such that 13 divides c_v. Then p splits in K.

Proof: Case 1: v does not divide 13

Proposition Let E_t be an elliptic curve over a quadratic field K with $E_t(K)_{tors} \simeq C_{13}$. Let v be a prime of K over a rational prime p such that 13 divides c_v. Then p splits in K.

Proof: Case 1: v does not divide 13

Let $x \in Y(K)$, v' be a prime of $\mathbb{Q}(\zeta_{13})^+$ above p. Denote by $\widetilde{y}$ the reduction of a $y \in X(K)$ mod v and denote by $\overline{y}$ the reduction of a $y \in X(\mathbb{Q}(\zeta_{13})^+)$ mod v'. Note $Y(\mathbb{Q}) = \emptyset$, so x is not defined over $\mathbb{Q}$.

Proposition Let E_t be an elliptic curve over a quadratic field K with $E_t(K)_{tors} \simeq C_{13}$. Let v be a prime of K over a rational prime p such that 13 divides c_v. Then p splits in K.

Proof: Case 1: v does not divide 13

Let $x \in Y(K)$, v' be a prime of $\mathbb{Q}(\zeta_{13})^+$ above p. Denote by $\widetilde{y}$ the reduction of a $y \in X(K)$ mod v and denote by $\overline{y}$ the reduction of a $y \in X(\mathbb{Q}(\zeta_{13})^+)$ mod v'. Note $Y(\mathbb{Q}) = \emptyset$, so x is not defined over $\mathbb{Q}$.

Let $\widetilde{x} = \overline{C}$ and $\widetilde{x^\sigma} = \overline{C_\sigma}$, for some cusps C and C_σ; $\overline{C}$ and $\overline{C_\sigma}$ are $\mathbb{F}_p$-rational by previous Lemma.

Proposition Let E_t be an elliptic curve over a quadratic field K with $E_t(K)_{tors} \simeq C_{13}$. Let v be a prime of K over a rational prime p such that 13 divides c_v. Then p splits in K.

Proof: Case 1: v does not divide 13

Let $x \in Y(K)$, v' be a prime of $\mathbb{Q}(\zeta_{13})^+$ above p. Denote by $\widetilde{y}$ the reduction of a $y \in X(K)$ mod v and denote by $\overline{y}$ the reduction of a $y \in X(\mathbb{Q}(\zeta_{13})^+)$ mod v'. Note $Y(\mathbb{Q}) = \emptyset$, so x is not defined over $\mathbb{Q}$.

Let $\widetilde{x} = \overline{C}$ and $\widetilde{x^\sigma} = \overline{C_\sigma}$, for some cusps C and C_σ; $\overline{C}$ and $\overline{C_\sigma}$ are $\mathbb{F}_p$-rational by previous Lemma.

If p is inert or ramified, it follows that

$$\overline{C_\sigma} = \widetilde{x^\sigma} = \widetilde{x}^{\mathrm{Frob}\, v} = \overline{C}^{\mathrm{Frob}\, v} = \overline{C}.$$

It follows that $[\widetilde{x} + \widetilde{x^\sigma} - 2\overline{C}] = 0$, and since, $[x + x^\sigma - 2C]$ is a $\mathbb{Q}(\zeta_{13})^+$-rational divisor class, and hence a torsion point, injectivity of reduction mod v' on $J(\mathbb{Q}(\zeta_{13})^+)_{tors}$ implies that $[x + x^\sigma - 2C] = 0$.

Thus $x + x^\sigma - 2C$ is a divisor of a rational function g, and since $x, x^\sigma \neq C$, g is of degree 2.

Thus $x + x^\sigma - 2C$ is a divisor of a rational function g, and since $x, x^\sigma \neq C$, g is of degree 2.

Since the hyperelliptic map is unique (up to an automorphism of $\mathbb{P}^1$), it follows that $g : X \to X/\langle \iota \rangle \simeq \mathbb{P}^1$ is the hyperelliptic map. It follows that C is fixed by ι, which is a contradiction.

Thus $x + x^\sigma - 2C$ is a divisor of a rational function g, and since $x, x^\sigma \neq C$, g is of degree 2.

Since the hyperelliptic map is unique (up to an automorphism of $\mathbb{P}^1$), it follows that $g : X \to X/\langle\iota\rangle \simeq \mathbb{P}^1$ is the hyperelliptic map. It follows that C is fixed by ι, which is a contradiction.

Case 2: v divides 13: All elliptic curves with a point of order 13 can be parameterized as

$$y^2 + a(t,s)xy + b(t,s)y = x^3 + b(t,s)x^2,$$

where $s = \sqrt{t^6 - 2t^5 + t^4 - 2t^3 + 6t^2 - 4t + 1}$, and $a(t,s)$ and $b(t,s)$ are rational functions in s and t. Thus the reduction type of E over a prime v over 13 depends only on the value of t mod 13. In all the cases when E_t has multiplicative reduction, we get that 13 splits in $\mathbb{Q}(s)$.

Proof of Krumm's conjecture

By the previous proposition we have, that if $v_{13}(c_v) > 0$, then $v \neq v^\sigma$. Since $E^\sigma \simeq E$, it follows that $c_v(E) = c_{v^\sigma}(E^\sigma) = c_{v^\sigma}(E)$.

Proof of Krumm's conjecture

By the previous proposition we have, that if $v_{13}(c_v) > 0$, then $v \neq v^\sigma$. Since $E^\sigma \simeq E$, it follows that $c_v(E) = c_{v^\sigma}(E^\sigma) = c_{v^\sigma}(E)$.

Hence $v_{13}(\prod_v c_v)$ is even.

Proof of Krumm's conjecture

By the previous proposition we have, that if $v_{13}(c_v) > 0$, then $v \neq v^\sigma$. Since $E^\sigma \simeq E$, it follows that $c_v(E) = c_{v^\sigma}(E^\sigma) = c_{v^\sigma}(E)$.

Hence $v_{13}(\prod_v c_v)$ is even.

Moreover, we prove that the elliptic curve

$$E_2 : y^2 + xy + y = x^3 - x^2 + \frac{-541 + 131\sqrt{17}}{2}x + 3624 - 879\sqrt{17}$$

is the only elliptic curve E over any quadratic field with C_{13} torsion such that $v_{13}(c_E) = 2$; for all other such curves $13^4 | c_E$.

Thank you for your attention!