Class invariants for genus 2

Part I: Kristin Lauter, Microsoft Research
Part II: Eyal Goren, McGill University

Conference on Abelian Varieties and Siegel Modular Forms
February 6, 2007

Elliptic curves with CM

$K = \mathbb{Q}(\sqrt{D})$ imaginary quadratic field

E an elliptic curve over a number field, $\mathcal{O}_K \hookrightarrow \mathrm{End}(E)$.

Constructing $E \Leftrightarrow$ find $j(E)$
$\Leftrightarrow$ compute the **Hilbert class polynomial**:

$$F_D(x) = \prod_{\frac{\{\tau:\, \mathbb{C}/\langle 1\ \tau\rangle \text{ has CM by } \mathcal{O}_K\}}{\mathrm{SL}_2(\mathbb{Z})}} (x - j(\tau)).$$

The points $j(\tau) \in \mathcal{A}_1(H_K)$ (and, in fact, generate H_K over K).

Elliptic curves with CM

$K = \mathbb{Q}(\sqrt{D})$ imaginary quadratic field

E an elliptic curve over a number field, $\mathcal{O}_K \hookrightarrow \mathrm{End}(E)$.

Constructing $E \Leftrightarrow$ find $j(E)$
$\Leftrightarrow$ compute the **Hilbert class polynomial**:

$$F_D(x) = \prod_{\frac{\{\tau\colon \mathbb{C}/\langle 1\ \tau\rangle \text{ has CM by } \mathcal{O}_K\}}{\mathrm{SL}_2(\mathbb{Z})}} (x - j(\tau)).$$

The points $j(\tau) \in \mathcal{A}_1(H_K)$ (and, in fact, generate H_K over K).

Elliptic curves with CM

$K = \mathbb{Q}(\sqrt{D})$ imaginary quadratic field

E an elliptic curve over a number field, $\mathcal{O}_K \hookrightarrow \mathrm{End}(E)$.

Constructing $E \Leftrightarrow$ find $j(E)$
$\Leftrightarrow$ compute the **Hilbert class polynomial**:

$$F_D(x) = \prod_{\frac{\{\tau\colon \mathbb{C}/\langle 1\ \tau\rangle \text{ has CM by } \mathcal{O}_K\}}{\mathrm{SL}_2(\mathbb{Z})}} (x - j(\tau)).$$

The points $j(\tau) \in \mathcal{A}_1(H_K)$ (and, in fact, generate H_K over K).

Properties of the Hilbert class polynomial

1. $F_D(x) \in \mathbb{Q}[x]$.
   This is the theory of complex multiplication; we are going over a complete set of Galois conjugates.
2. $F_D(x) \in \mathbb{Z}[x]$.

   no denominators $\Leftrightarrow$ every singular moduli is an algebraic integer
   $\Leftrightarrow$ every CM elliptic curve has potentially good reduction everywhere.

Properties of the Hilbert class polynomial

1. $F_D(x) \in \mathbb{Q}[x]$.
   This is the theory of complex multiplication; we are going over a complete set of Galois conjugates.
2. $F_D(x) \in \mathbb{Z}[x]$.

   no denominators $\Leftrightarrow$ every singular moduli is an algebraic integer
   $\Leftrightarrow$ every CM elliptic curve has potentially good reduction everywhere.

Properties of the Hilbert class polynomial

1. $F_D(x) \in \mathbb{Q}[x]$.
   This is the theory of complex multiplication; we are going over a complete set of Galois conjugates.
2. $F_D(x) \in \mathbb{Z}[x]$.

   no denominators $\Leftrightarrow$ every singular moduli is an algebraic integer
   $\Leftrightarrow$ every CM elliptic curve has potentially good reduction everywhere.

Properties of the Hilbert class polynomial

1. $F_D(x) \in \mathbb{Q}[x]$.
   This is the theory of complex multiplication; we are going over a complete set of Galois conjugates.
2. $F_D(x) \in \mathbb{Z}[x]$.

   no denominators $\Leftrightarrow$ every singular moduli is an algebraic integer
   $\Leftrightarrow$ every CM elliptic curve has potentially good reduction everywhere.

Properties of the Hilbert class polynomial

1. $F_D(x) \in \mathbb{Q}[x]$.
   This is the theory of complex multiplication; we are going over a complete set of Galois conjugates.
2. $F_D(x) \in \mathbb{Z}[x]$.

   no denominators $\Leftrightarrow$ every singular moduli is an algebraic integer
   $\Leftrightarrow$ every CM elliptic curve has potentially good reduction everywhere.

Calculating the Hilbert class polynomial

Various methods:

1. Complex analytic (Atkin-Morain)

-for each ideal class in $\mathcal{O}_K$, evaluate modular j-function on complex lattice associated to the ideal

-in practice this is done by running through reduced, primitive, binary quadratic forms of discriminant D

-evaluate with sufficiently high precision (roughly $\sqrt{D}log(D)^2$ bits)

-form the minimal polynomial by multiplying the linear factors and round the coefficients to integers

2. Chinese Remainder Theorem (Agashe-L-Venkatesan)
3. p-adic method (Couveignes-Henocq, Broker)

Calculating the Hilbert class polynomial

Various methods:

1. Complex analytic (Atkin-Morain)

-for each ideal class in $\mathcal{O}_K$, evaluate modular j-function on complex lattice associated to the ideal

-in practice this is done by running through reduced, primitive, binary quadratic forms of discriminant D

-evaluate with sufficiently high precision (roughly $\sqrt{D}log(D)^2$ bits)

-form the minimal polynomial by multiplying the linear factors and round the coefficients to integers

2. Chinese Remainder Theorem (Agashe-L-Venkatesan)
3. p-adic method (Couveignes-Henocq, Broker)

Calculating the Hilbert class polynomial

Various methods:

1. Complex analytic (Atkin-Morain)

-for each ideal class in $\mathcal{O}_K$, evaluate modular j-function on complex lattice associated to the ideal

-in practice this is done by running through reduced, primitive, binary quadratic forms of discriminant D

-evaluate with sufficiently high precision (roughly $\sqrt{D}log(D)^2$ bits)

-form the minimal polynomial by multiplying the linear factors and round the coefficients to integers

2. Chinese Remainder Theorem (Agashe-L-Venkatesan)
3. p-adic method (Couveignes-Henocq, Broker)

Calculating the Hilbert class polynomial

Various methods:

1. Complex analytic (Atkin-Morain)

-for each ideal class in $\mathcal{O}_K$, evaluate modular j-function on complex lattice associated to the ideal

-in practice this is done by running through reduced, primitive, binary quadratic forms of discriminant D

-evaluate with sufficiently high precision (roughly $\sqrt{D}log(D)^2$ bits)

-form the minimal polynomial by multiplying the linear factors and round the coefficients to integers

2. Chinese Remainder Theorem (Agashe-L-Venkatesan)
3. p-adic method (Couveignes-Henocq, Broker)

Calculating the Hilbert class polynomial

Various methods:

1. Complex analytic (Atkin-Morain)

-for each ideal class in $\mathcal{O}_K$, evaluate modular j-function on complex lattice associated to the ideal

-in practice this is done by running through reduced, primitive, binary quadratic forms of discriminant D

-evaluate with sufficiently high precision (roughly $\sqrt{D}log(D)^2$ bits)

-form the minimal polynomial by multiplying the linear factors and round the coefficients to integers

2. Chinese Remainder Theorem (Agashe-L-Venkatesan)
3. p-adic method (Couveignes-Henocq, Broker)

Calculating the Hilbert class polynomial

Various methods:

1. Complex analytic (Atkin-Morain)

-for each ideal class in $\mathcal{O}_K$, evaluate modular j-function on complex lattice associated to the ideal

-in practice this is done by running through reduced, primitive, binary quadratic forms of discriminant D

-evaluate with sufficiently high precision (roughly $\sqrt{D}log(D)^2$ bits)

-form the minimal polynomial by multiplying the linear factors and round the coefficients to integers

2. Chinese Remainder Theorem (Agashe-L-Venkatesan)
3. p-adic method (Couveignes-Henocq, Broker)

Calculating the Hilbert class polynomial

Various methods:

1. Complex analytic (Atkin-Morain)

-for each ideal class in $\mathcal{O}_K$, evaluate modular j-function on complex lattice associated to the ideal

-in practice this is done by running through reduced, primitive, binary quadratic forms of discriminant D

-evaluate with sufficiently high precision (roughly $\sqrt{D}log(D)^2$ bits)

-form the minimal polynomial by multiplying the linear factors and round the coefficients to integers

2. Chinese Remainder Theorem (Agashe-L-Venkatesan)
3. p-adic method (Couveignes-Henocq, Broker)

Cryptographic Motivation

Elliptic Curve Cryptosystems

ECDLP (Elliptic Curve Discrete Logarithm Problem): Given two points on $E(\mathbb{F}_p)$, P and $Q = mP$, find m.

Best known algorithms are exponential in largest prime factor of the group size.

p can be taken to be of size 2^{256}
need elliptic curve with large prime order, $N = p + 1 - t$
Use theory of CM with $K = \mathbb{Q}(\sqrt{D})$, where $D = t^2 - 4p$

Cryptographic Motivation

Elliptic Curve Cryptosystems

ECDLP (Elliptic Curve Discrete Logarithm Problem): Given two points on $E(\mathbb{F}_p)$, P and $Q = mP$, find m.

Best known algorithms are exponential in largest prime factor of the group size.

p can be taken to be of size 2^{256}
need elliptic curve with large prime order, $N = p + 1 - t$
Use theory of CM with $K = \mathbb{Q}(\sqrt{D})$, where $D = t^2 - 4p$

Cryptographic Motivation

Elliptic Curve Cryptosystems

ECDLP (Elliptic Curve Discrete Logarithm Problem): Given two points on $E(\mathbb{F}_p)$, P and $Q = mP$, find m.

Best known algorithms are exponential in largest prime factor of the group size.

p can be taken to be of size 2^{256}
need elliptic curve with large prime order, $N = p + 1 - t$
Use theory of CM with $K = \mathbb{Q}(\sqrt{D})$, where $D = t^2 - 4p$

Cryptographic Motivation

Elliptic Curve Cryptosystems

ECDLP (Elliptic Curve Discrete Logarithm Problem): Given two points on $E(\mathbb{F}_p)$, P and $Q = mP$, find m.

Best known algorithms are exponential in largest prime factor of the group size.

p can be taken to be of size 2^{256}

need elliptic curve with large prime order, $N = p + 1 - t$

Use theory of CM with $K = \mathbb{Q}(\sqrt{D})$, where $D = t^2 - 4p$

Cryptographic Motivation

Elliptic Curve Cryptosystems

ECDLP (Elliptic Curve Discrete Logarithm Problem): Given two points on $E(\mathbb{F}_p)$, P and $Q = mP$, find m.

Best known algorithms are exponential in largest prime factor of the group size.

p can be taken to be of size 2^{256}
need elliptic curve with large prime order, $N = p + 1 - t$
Use theory of CM with $K = \mathbb{Q}(\sqrt{D})$, where $D = t^2 - 4p$

Cryptographic Motivation

Elliptic Curve Cryptosystems

ECDLP (Elliptic Curve Discrete Logarithm Problem): Given two points on $E(\mathbb{F}_p)$, P and $Q = mP$, find m.

Best known algorithms are exponential in largest prime factor of the group size.

p can be taken to be of size 2^{256}
need elliptic curve with large prime order, $N = p + 1 - t$
Use theory of CM with $K = \mathbb{Q}(\sqrt{D})$, where $D = t^2 - 4p$

Constructing genus 2 curves for cryptography

Discrete log problem on the Jacobian of a genus 2 hyperelliptic curve over large prime fields F_p can also be used in cryptography

Key exchange or digital signatures, here p of size 2^{128}

need group of large prime order (some small cofactors OK)

No good point-counting algorithms in large characteristic, so we need to construct curves with a known order using complex multiplication techniques. Same idea as above: given a desired number of points and zeta function for the Jacobian over $\mathbb{F}_p$, this determines a quartic CM field K.

Constructing genus 2 curves for cryptography

Discrete log problem on the Jacobian of a genus 2 hyperelliptic curve over large prime fields F_p can also be used in cryptography

Key exchange or digital signatures, here p of size 2^{128}

need group of large prime order (some small cofactors OK)

No good point-counting algorithms in large characteristic, so we need to construct curves with a known order using complex multiplication techniques. Same idea as above: given a desired number of points and zeta function for the Jacobian over $\mathbb{F}_p$, this determines a quartic CM field K.

Constructing genus 2 curves for cryptography

Discrete log problem on the Jacobian of a genus 2 hyperelliptic curve over large prime fields F_p can also be used in cryptography

Key exchange or digital signatures, here p of size 2^{128}

need group of large prime order (some small cofactors OK)

No good point-counting algorithms in large characteristic, so we need to construct curves with a known order using complex multiplication techniques. Same idea as above: given a desired number of points and zeta function for the Jacobian over $\mathbb{F}_p$, this determines a quartic CM field K.

Constructing genus 2 curves for cryptography

Discrete log problem on the Jacobian of a genus 2 hyperelliptic curve over large prime fields F_p can also be used in cryptography

Key exchange or digital signatures, here p of size 2^{128}

need group of large prime order (some small cofactors OK)

No good point-counting algorithms in large characteristic, so we need to construct curves with a known order using complex multiplication techniques. Same idea as above: given a desired number of points and zeta function for the Jacobian over $\mathbb{F}_p$, this determines a quartic CM field K.

Genus 2 curves with CM

K = quartic primitive CM field.

K^* = the reflex field (for some fixed CM type).

Definition

A curve C over a number field has CM by $\mathcal{O}_K$ if $\mathcal{O}_K$ embeds in the endomorphism ring of $\mathrm{Jac}(C)$ (after base change). We let $x_C \in \mathcal{A}_2(H_{K^*})$ be the moduli point of $(\mathrm{Jac}(C), \Theta)$.

Igusa proved that $\mathcal{A}_2(\mathbb{C}) \sim \mathbb{C}^3$ and gave 3 generators h_1, h_2, h_3, the "absolute Igusa invariants", for the function field.

Up to isomorphism, the curve can be reconstructed from its invariants (Mestre's algorithm). It can fail to be defined over the field of definition of the invariants.

Genus 2 curves with CM

$K =$ quartic primitive CM field.

$K^* =$ the reflex field (for some fixed CM type).

Definition

A curve C over a number field has CM by $\mathcal{O}_K$ if $\mathcal{O}_K$ embeds in the endomorphism ring of $\mathrm{Jac}(C)$ (after base change). We let $x_C \in \mathcal{A}_2(H_{K^*})$ be the moduli point of $(\mathrm{Jac}(C), \Theta)$.

Igusa proved that $\mathcal{A}_2(\mathbb{C}) \sim \mathbb{C}^3$ and gave 3 generators h_1, h_2, h_3, the "absolute Igusa invariants", for the function field.

Up to isomorphism, the curve can be reconstructed from its invariants (Mestre's algorithm). It can fail to be defined over the field of definition of the invariants.

Genus 2 curves with CM

$K =$ quartic primitive CM field.

$K^* =$ the reflex field (for some fixed CM type).

Definition

A curve C over a number field has CM by $\mathcal{O}_K$ if $\mathcal{O}_K$ embeds in the endomorphism ring of $\mathrm{Jac}(C)$ (after base change). We let $x_C \in \mathcal{A}_2(H_{K^*})$ be the moduli point of $(\mathrm{Jac}(C), \Theta)$.

Igusa proved that $\mathcal{A}_2(\mathbb{C}) \sim \mathbb{C}^3$ and gave 3 generators h_1, h_2, h_3, the "absolute Igusa invariants", for the function field.

Up to isomorphism, the curve can be reconstructed from its invariants (Mestre's algorithm). It can fail to be defined over the field of definition of the invariants.

Genus 2 curves with CM

$K =$ quartic primitive CM field.

$K^* =$ the reflex field (for some fixed CM type).

Definition

A curve C over a number field has CM by $\mathcal{O}_K$ if $\mathcal{O}_K$ embeds in the endomorphism ring of $\mathrm{Jac}(C)$ (after base change). We let $x_C \in \mathcal{A}_2(H_{K^*})$ be the moduli point of $(\mathrm{Jac}(C), \Theta)$.

Igusa proved that $\mathcal{A}_2(\mathbb{C}) \sim \mathbb{C}^3$ and gave 3 generators h_1, h_2, h_3, the "absolute Igusa invariants", for the function field.

Up to isomorphism, the curve can be reconstructed from its invariants (Mestre's algorithm). It can fail to be defined over the field of definition of the invariants.

Igusa's invariants

$$h_1 = 2 \cdot 3^5 \chi_{10}^{-6} \chi_{12}^5,$$

$$h_2 = 2^{-3} \cdot 3^3 \psi_4 \chi_{10}^{-4} \chi_{12}^3,$$

$$h_3 = 2^{-5} \cdot 3 \psi_6 \chi_{10}^{-3} \chi_{12}^2 + 2^2 \cdot 3 \psi_4 \chi_{10}^{-4} \chi_{12}^3.$$

Definition

The Igusa class polynomials

$$F_i(x) = \prod_{\frac{\{\tau:\, \mathbb{C}^2/\langle \mathrm{I}_2\ \tau\rangle \text{ has CM by } \mathcal{O}_K\}}{\mathrm{Sp}_4(\mathbb{Z})}} (x - h_i(\tau)), \qquad i = 1, 2, 3.$$

1. $F_i(x) \in \mathbb{Q}[x]$, by the theory of complex multiplication.
2. $F_i(x) \in \mathbb{Z}[x]$??!

No!

Definition

The Igusa class polynomials

$$F_i(x) = \prod_{\frac{\{\tau:\ \mathbb{C}^2/\langle \mathrm{I}_2\ \tau\rangle \text{ has CM by } \mathcal{O}_K\}}{\mathrm{Sp}_4(\mathbb{Z})}} (x - h_i(\tau)), \qquad i = 1, 2, 3.$$

1. $F_i(x) \in \mathbb{Q}[x]$, by the theory of complex multiplication.
2. $F_i(x) \in \mathbb{Z}[x]$??!.

No!

Definition

The Igusa class polynomials

$$F_i(x) = \prod_{\frac{\{\tau:\, \mathbb{C}^2/\langle \mathrm{I}_2\ \tau\rangle \text{ has CM by } \mathcal{O}_K\}}{\mathrm{Sp}_4(\mathbb{Z})}} (x - h_i(\tau)), \qquad i = 1, 2, 3.$$

1. $F_i(x) \in \mathbb{Q}[x]$, by the theory of complex multiplication.
2. $F_i(x) \in \mathbb{Z}[x]$??!.

No!

Definition

The Igusa class polynomials

$$F_i(x) = \prod_{\frac{\{\tau:\, \mathbb{C}^2/\langle \mathrm{I}_2\ \tau\rangle \text{ has CM by } \mathcal{O}_K\}}{\mathrm{Sp}_4(\mathbb{Z})}} (x - h_i(\tau)), \qquad i = 1, 2, 3.$$

1. $F_i(x) \in \mathbb{Q}[x]$, by the theory of complex multiplication.
2. $F_i(x) \in \mathbb{Z}[x]$??!.

No!

Calculating Igusa Class polynomials

Various methods:

1. Complex analytic (Spallek '92, van Wamelen '99 (over $\mathbb{Q}$), Weng '00, Cohn-L '01) ($h_{K^+} = 1$)

-for each ideal class in $\mathcal{O}_K$, evaluate Igusa's modular functions on period lattice associated to the ideal class and polarization

-evaluate with sufficiently high precision (how much?)

-form the minimal polynomial by multiplying the linear factors and (hopefully) recognize rational cofficients using continued fractions algorithm

2. Chinese Remainder Theorem (Eisentraeger-L)
3. p-adic method (Gaudry-Houtmann-Kohel-Ritzenthaler-Weng)

Calculating Igusa Class polynomials

Various methods:
1. Complex analytic (Spallek '92, van Wamelen '99 (over $\mathbb{Q}$), Weng '00, Cohn-L '01) ($h_{K^+} = 1$)

-for each ideal class in $\mathcal{O}_K$, evaluate Igusa's modular functions on period lattice associated to the ideal class and polarization

-evaluate with sufficiently high precision (how much?)

-form the minimal polynomial by multiplying the linear factors and (hopefully) recognize rational cofficients using continued fractions algorithm

2. Chinese Remainder Theorem (Eisentraeger-L)
3. p-adic method (Gaudry-Houtmann-Kohel-Ritzenthaler-Weng)

Calculating Igusa Class polynomials

Various methods:
1. Complex analytic (Spallek '92, van Wamelen '99 (over $\mathbb{Q}$), Weng '00, Cohn-L '01) ($h_{K^+} = 1$)

-for each ideal class in $\mathcal{O}_K$, evaluate Igusa's modular functions on period lattice associated to the ideal class and polarization

-evaluate with sufficiently high precision (how much?)

-form the minimal polynomial by multiplying the linear factors and (hopefully) recognize rational cofficients using continued fractions algorithm

2. Chinese Remainder Theorem (Eisentraeger-L)
3. p-adic method (Gaudry-Houtmann-Kohel-Ritzenthaler-Weng)

Calculating Igusa Class polynomials

Various methods:
1. Complex analytic (Spallek '92, van Wamelen '99 (over $\mathbb{Q}$), Weng '00, Cohn-L '01) ($h_{K^+} = 1$)

-for each ideal class in $\mathcal{O}_K$, evaluate Igusa's modular functions on period lattice associated to the ideal class and polarization

-evaluate with sufficiently high precision (how much?)

-form the minimal polynomial by multiplying the linear factors and (hopefully) recognize rational cofficients using continued fractions algorithm

2. Chinese Remainder Theorem (Eisentraeger-L)
3. p-adic method (Gaudry-Houtmann-Kohel-Ritzenthaler-Weng)

Calculating Igusa Class polynomials

Various methods:
1. Complex analytic (Spallek '92, van Wamelen '99 (over $\mathbb{Q}$), Weng '00, Cohn-L '01) ($h_{K^+} = 1$)

-for each ideal class in $\mathcal{O}_K$, evaluate Igusa's modular functions on period lattice associated to the ideal class and polarization

-evaluate with sufficiently high precision (how much?)

-form the minimal polynomial by multiplying the linear factors and (hopefully) recognize rational cofficients using continued fractions algorithm

2. Chinese Remainder Theorem (Eisentraeger-L)
3. p-adic method (Gaudry-Houtmann-Kohel-Ritzenthaler-Weng)

Calculating Igusa Class polynomials

Various methods:
1. Complex analytic (Spallek '92, van Wamelen '99 (over $\mathbb{Q}$), Weng '00, Cohn-L '01) ($h_{K^+} = 1$)

-for each ideal class in $\mathcal{O}_K$, evaluate Igusa's modular functions on period lattice associated to the ideal class and polarization

-evaluate with sufficiently high precision (how much?)

-form the minimal polynomial by multiplying the linear factors and (hopefully) recognize rational cofficients using continued fractions algorithm

2. Chinese Remainder Theorem (Eisentraeger-L)
3. p-adic method (Gaudry-Houtmann-Kohel-Ritzenthaler-Weng)

Example

$K = \mathbb{Q}[x]/(x^4 + 50x^2 + 93)$ non-normal quartic CM field.

$h_K = 4$

Generated by $i\sqrt{25 + 2\sqrt{133}}$ over totally real subfield $K^+ = \mathbb{Q}(\sqrt{133})$.

$d_K =$ discriminant of $K = 3 \cdot 31 \cdot 133^2$.

The reflex field of K^* is the quartic CM field $K^* = \mathbb{Q}[x]/(x^4 + 100x^2 + 2128)$, and it also has class number 4.
The first class polynomial $F_1(X)$ for K is:

$$F_1(X) = X^8 +$$
$$(1041267141265383834470066376076324878559188075169214718620644562742786358262348341096508075804599$$
$$1439699844537752039989836959475480039725985450531913452727685520366992417930481289340643367738572714561898$$
$$2352381068613549757086042044564516074208093384753878388383997147217922X^7 -$$
$$1214939779396317811262782102262089 2$$
$$4540413608767159829695347294040442570821432287697658903718776135501480690221738293322842166444538516148677$$
$$8621642565344297081586957670592740919978813590684188959957559943995233875289149403700489027842584764660922$$
$$3829932461236811798235188297728X^6 +$$
$$7383904997141634980607641452730031663337889747506381230205379941950662 4$$
$$9251812916596445900943280736278717237350759409045470486566299533568060028209655446852220400385271017191828$$
$$2288108439856522784301574892743531783281312324613949422023041187999846781654936602338763464742349431007852$$
$$4432X^5 +$$
$$1357207258461000262735106409656244080068778990606962562095457227581540708992905492484722140534661 7$$
$$8130334882154668632791244726371290934187616015929225806173084913934429418610855648493194839702426010467395$$
$$4586024623515424709268737708970627134380928657846514322488728304186508199618879413397517590329798164 48X^4 -$$
$$2064541907189909406231906095021518513282252383433786632489981649009993051911532529174569178509954174241284$$
$$5065909310167001379732482606212817730848758983943571197938282916313941206563110208509856289122139170762118$$
$$6733170257389221578842790790536175427848548886553551634053100728321789568362872897268981614772224X^3 -$$
$$129312493$$
$$7479769249061778818022624358655510743462873298439586515036372146763574796362009513855612419032661986690064$$
$$4274554269687399107364202173634493779363264596654252667526655309675594052452885344755398557406456478604366$$
$$9900881042665574443409015280387939430971217614297104566348752262793311583985309563588143414632461107 2X^2 -$$
$$1751631054042862854045582423881782324011347856494871100374355732064705511136577792596014084092595288225412$$
$$2655958399190812186717037021899314074325292680046412088549592986428095578646570526189473144725821984588076$$
$$2126346415980671910863549185136706731565851225891478828311792074540631305421890310594326611176095702219390$$
$$+1604398176398171965083954530143587467864124228892266410893720503328183568724268331605647208243792414122$$
$$9829809436209614247347445529927942891679831852123345009452309770705794789072204482562816034616210685390885$$
$$6437672763292720798162365206307314646594632579281296420073078445474401380548434319635226631450753809199086$$
$$365137199566422016)/$$
$$1654971517931923355856381943338076188857572258507293513925701338688430849661907853436240641539 9$$
$$3060472421943063977491964645435818434816422816448520354952124186248583885336013832737212668433932405635280$$
$$7669880275984557132109905292220437178968384 1$$

The denominator factors as:

$$7^{48} \cdot 11^{72} \cdot 19^{24} \cdot 23^{12} \cdot 29^{12} \cdot 83^{12} \cdot 89^{12} \cdot 167^{12}.$$

F_2, F_3 have the same primes in their denominators.

The polynomials were computed using PARI with 1000 digits of precision in about 8 hours each on an Intel Pentium 4, 2.2GHZ, 512MB memory.

Conjecture (L. '03). Primes in the denominators are bounded by the discriminant d_K and divide $d_K - x^2$, for some integer $x < \sqrt{d_K}$.

The main problems

1. Find an explicit set of rational primes S such that $F_i(x) \in \mathbb{Z}[S^{-1}][x]$.
2. Find an optimal explicit set of primes S_τ such that $h_i(\tau)$ is S_τ-integral.
3. Factor $h_i(\tau)$.

The main problems

1. Find an explicit set of rational primes S such that $F_i(x) \in \mathbb{Z}[S^{-1}][x]$.
2. Find an optimal explicit set of primes S_τ such that $h_i(\tau)$ is S_τ-integral.
3. Factor $h_i(\tau)$.

The main problems

1. Find an explicit set of rational primes S such that $F_i(x) \in \mathbb{Z}[S^{-1}][x]$.
2. Find an optimal explicit set of primes S_τ such that $h_i(\tau)$ is S_τ-integral.
3. Factor $h_i(\tau)$.

The main problems

1. Find an explicit set of rational primes S such that $F_i(x) \in \mathbb{Z}[S^{-1}][x]$.
2. Find an optimal explicit set of primes S_τ such that $h_i(\tau)$ is S_τ-integral.
3. Factor $h_i(\tau)$.

The main problems

1. Find an explicit set of rational primes S such that $F_i(x) \in \mathbb{Z}[S^{-1}][x]$.
2. Find an optimal explicit set of primes S_τ such that $h_i(\tau)$ is S_τ-integral.
3. Factor $h_i(\tau)$.

The main problems

1. Find an explicit set of rational primes S such that $F_i(x) \in \mathbb{Z}[S^{-1}][x]$.
2. Find an optimal explicit set of primes S_τ such that $h_i(\tau)$ is S_τ-integral.
3. Factor $h_i(\tau)$.

After base-change, may assume C has a stable model $\mathscr{C}$ over $\mathcal{O}_M$, $M \supset H_{K^*}$.

The denominator of each h_i is a power of

$$\Delta = 2^{-12} \prod_{10 \text{ even char.} \left[\begin{smallmatrix}\epsilon\\ \epsilon'\end{smallmatrix}\right]} \Theta\left[\begin{smallmatrix}\epsilon\\ \epsilon'\end{smallmatrix}\right]^2(\tau).$$

(A Siegel modular form of level 1 and weight 10 on $\mathrm{Sp}_4(\mathbb{Z})\backslash\mathfrak{H}_2$).

Key point

The divisor of Δ is "arithmetically" the locus of $(E_1 \times E_2, \lambda_1 \times \lambda_2)$ (canonically polarized products of elliptic curves).

Hence, $\mathrm{val}_{\mathfrak{p}}(h_i(\tau)) < 0 \Rightarrow \mathscr{C} \mod \mathfrak{p}$ is two supersingular elliptic curves crossing transversely at their origin.

We call then $p = \mathfrak{p} \cap \mathbb{Z}$ an evil prime for K.

After base-change, may assume C has a stable model $\mathscr{C}$ over $\mathcal{O}_M$, $M \supset H_{K^*}$.

The denominator of each h_i is a power of

$$\Delta = 2^{-12} \prod_{10 \text{ even char.} \left[\begin{smallmatrix}\epsilon\\ \epsilon'\end{smallmatrix}\right]} \Theta\left[\begin{smallmatrix}\epsilon\\ \epsilon'\end{smallmatrix}\right]^2(\tau).$$

(A Siegel modular form of level 1 and weight 10 on $\mathrm{Sp}_4(\mathbb{Z})\backslash\mathfrak{H}_2$).

Key point

The divisor of Δ is "arithmetically" the locus of $(E_1 \times E_2, \lambda_1 \times \lambda_2)$ (canonically polarized products of elliptic curves).
Hence, $\mathrm{val}_{\mathfrak{p}}(h_i(\tau)) < 0 \Rightarrow \mathscr{C} \mod \mathfrak{p}$ is two supersingular elliptic curves crossing transversely at their origin.
We call then $p = \mathfrak{p} \cap \mathbb{Z}$ an evil prime for K.

After base-change, may assume C has a stable model $\mathscr{C}$ over $\mathcal{O}_M$, $M \supset H_{K^*}$.

The denominator of each h_i is a power of

$$\Delta = 2^{-12} \prod_{10 \text{ even char.} \left[\begin{smallmatrix}\epsilon \\ \epsilon'\end{smallmatrix}\right]} \Theta\left[\begin{smallmatrix}\epsilon \\ \epsilon'\end{smallmatrix}\right]^2(\tau).$$

(A Siegel modular form of level 1 and weight 10 on $\mathrm{Sp}_4(\mathbb{Z})\backslash\mathfrak{H}_2$).

Key point

The divisor of Δ is "arithmetically" the locus of $(E_1 \times E_2, \lambda_1 \times \lambda_2)$ (canonically polarized products of elliptic curves).
Hence, $\mathrm{val}_{\mathfrak{p}}(h_i(\tau)) < 0 \Rightarrow \mathscr{C} \mod \mathfrak{p}$ is two supersingular elliptic curves crossing transversely at their origin.
We call then $p = \mathfrak{p} \cap \mathbb{Z}$ an evil prime for K.

After base-change, may assume C has a stable model $\mathscr{C}$ over $\mathcal{O}_M$, $M \supset H_{K^*}$.

The denominator of each h_i is a power of

$$\Delta = 2^{-12} \prod_{10 \text{ even char.} \left[\begin{smallmatrix}\epsilon \\ \epsilon'\end{smallmatrix}\right]} \Theta\left[\begin{smallmatrix}\epsilon \\ \epsilon'\end{smallmatrix}\right]^2(\tau).$$

(A Siegel modular form of level 1 and weight 10 on $\mathrm{Sp}_4(\mathbb{Z})\backslash\mathfrak{H}_2$).

Key point

The divisor of Δ is "arithmetically" the locus of $(E_1 \times E_2, \lambda_1 \times \lambda_2)$ (canonically polarized products of elliptic curves).

Hence, $\mathrm{val}_{\mathfrak{p}}(h_i(\tau)) < 0 \Rightarrow \mathscr{C} \mod \mathfrak{p}$ is two supersingular elliptic curves crossing transversely at their origin.

We call then $p = \mathfrak{p} \cap \mathbb{Z}$ an evil prime for K.

After base-change, may assume C has a stable model $\mathscr{C}$ over $\mathcal{O}_M$, $M \supset H_{K^*}$.

The denominator of each h_i is a power of

$$\Delta = 2^{-12} \prod_{10 \text{ even char.} \left[\begin{smallmatrix}\epsilon\\ \epsilon'\end{smallmatrix}\right]} \Theta\left[\begin{smallmatrix}\epsilon\\ \epsilon'\end{smallmatrix}\right]^2(\tau).$$

(A Siegel modular form of level 1 and weight 10 on $\mathrm{Sp}_4(\mathbb{Z})\backslash\mathfrak{H}_2$).

Key point

The divisor of Δ is "arithmetically" the locus of $(E_1 \times E_2, \lambda_1 \times \lambda_2)$ (canonically polarized products of elliptic curves).

Hence, $\mathrm{val}_{\mathfrak{p}}(h_i(\tau)) < 0 \Rightarrow \mathscr{C} \mod \mathfrak{p}$ is two supersingular elliptic curves crossing transversely at their origin.

We call then $p = \mathfrak{p} \cap \mathbb{Z}$ an evil prime for K.

After base-change, may assume C has a stable model $\mathscr{C}$ over $\mathcal{O}_M$, $M \supset H_{K^*}$.

The denominator of each h_i is a power of

$$\Delta = 2^{-12} \prod_{10 \text{ even char.} \left[\begin{smallmatrix}\epsilon \\ \epsilon'\end{smallmatrix}\right]} \Theta\left[\begin{smallmatrix}\epsilon \\ \epsilon'\end{smallmatrix}\right]^2(\tau).$$

(A Siegel modular form of level 1 and weight 10 on $\mathrm{Sp}_4(\mathbb{Z})\backslash\mathfrak{H}_2$).

Key point

The divisor of Δ is "arithmetically" the locus of $(E_1 \times E_2, \lambda_1 \times \lambda_2)$ (canonically polarized products of elliptic curves).
Hence, $\mathrm{val}_{\mathfrak{p}}(h_i(\tau)) < 0 \Rightarrow \mathscr{C} \mod \mathfrak{p}$ is two supersingular elliptic curves crossing transversely at their origin.
We call then $p = \mathfrak{p} \cap \mathbb{Z}$ an evil prime for K.

Bound on evil primes

Theorem (G.-Lauter, Annales Inst. Fourier 2007)

Write $K = \mathbb{Q}(\sqrt{d})(\sqrt{r})$, $d > 0$ a $\square$-free integer, $r = a + b\sqrt{d}$, $a, b \in \mathbb{Z}$ totally negative. If p is an evil prime then

$$p \leq d^2 \operatorname{Tr}(r)^2.$$

The superspecial primes decompose in K in a certain way (Goren '96) and so for example in the Galois cyclic case, $p\mathcal{O}_K = \mathfrak{P}_1\mathfrak{P}_2$.

Thus there are an infinite number of superspecial primes, so the key point is the product polarization.

Bound on evil primes

Theorem (G.-Lauter, Annales Inst. Fourier 2007)

Write $K = \mathbb{Q}(\sqrt{d})(\sqrt{r})$, $d > 0$ a $\square$-free integer, $r = a + b\sqrt{d}$, $a, b \in \mathbb{Z}$ totally negative. If p is an evil prime then

$$p \leq d^2 \operatorname{Tr}(r)^2.$$

The superspecial primes decompose in K in a certain way (Goren '96) and so for example in the Galois cyclic case, $p\mathcal{O}_K = \mathfrak{P}_1\mathfrak{P}_2$.

Thus there are an infinite number of superspecial primes, so the key point is the product polarization.

Bound on evil primes

Theorem (G.-Lauter, Annales Inst. Fourier 2007)

Write $K = \mathbb{Q}(\sqrt{d})(\sqrt{r})$, $d > 0$ a $\square$-free integer, $r = a + b\sqrt{d}$, $a, b \in \mathbb{Z}$ totally negative. If p is an evil prime then

$$p \leq d^2 \operatorname{Tr}(r)^2.$$

The superspecial primes decompose in K in a certain way (Goren '96) and so for example in the Galois cyclic case, $p\mathcal{O}_K = \mathfrak{P}_1\mathfrak{P}_2$.

Thus there are an infinite number of superspecial primes, so the key point is the product polarization.

Class invariants

Explicit construction of units in extension of number fields is motivated by Stark's conjectures and explicit class field theory.

Construction (DeShalit-G., Annales Inst. Fourier 1997):

$$(\mathfrak{a}, \mathfrak{b}) \in Cl(K) \times CL(K) \rightsquigarrow u(\Phi; \mathfrak{a}, \mathfrak{b}) \in H_{K^*}.$$

This is done by evaluating Δ on period matrices associated to $\mathcal{O}_K, \mathfrak{a}, \mathfrak{b}, \mathfrak{ab}$. These invariants have very nice properties. ("Behave like units", "nice" Galois action ...)

Key point

If $u(\Phi; \mathfrak{a}, \mathfrak{b})$ is not a unit at $\mathfrak{p}$ then p is an evil prime.

Class invariants

Explicit construction of units in extension of number fields is motivated by Stark's conjectures and explicit class field theory.

Construction (DeShalit-G., Annales Inst. Fourier 1997):

$$(\mathfrak{a}, \mathfrak{b}) \in Cl(K) \times CL(K) \rightsquigarrow u(\Phi; \mathfrak{a}, \mathfrak{b}) \in H_{K^*}.$$

This is done by evaluating Δ on period matrices associated to $\mathcal{O}_K, \mathfrak{a}, \mathfrak{b}, \mathfrak{ab}$. These invariants have very nice properties. ("Behave like units", "nice" Galois action ...)

Key point

If $u(\Phi; \mathfrak{a}, \mathfrak{b})$ is not a unit at $\mathfrak{p}$ then p is an evil prime.

Class invariants

Explicit construction of units in extension of number fields is motivated by Stark's conjectures and explicit class field theory.

Construction (DeShalit-G., Annales Inst. Fourier 1997):

$$(\mathfrak{a}, \mathfrak{b}) \in Cl(K) \times CL(K) \rightsquigarrow u(\Phi; \mathfrak{a}, \mathfrak{b}) \in H_{K^*}.$$

This is done by evaluating Δ on period matrices associated to $\mathcal{O}_K, \mathfrak{a}, \mathfrak{b}, \mathfrak{ab}$. These invariants have very nice properties. ("Behave like units", "nice" Galois action ...)

Key point

If $u(\Phi; \mathfrak{a}, \mathfrak{b})$ is not a unit at $\mathfrak{p}$ then p is an evil prime.

Elements of small norm commute

Lemma

Let $R \subseteq B_{p,\infty}$ be a maximal order and $x_1, x_2 \in R$ elements so that $\mathrm{Norm}(x_i) < \frac{\sqrt{p}}{2}$ then $x_1 x_2 = x_2 x_1$.

Proof.

If not, then we get a full lattice spanned by $1, x_1, x_2, x_1 x_2$. Proceed by evaluating its volume. □

Elements of small norm commute

Lemma

Let $R \subseteq B_{p,\infty}$ be a maximal order and $x_1, x_2 \in R$ elements so that $\mathrm{Norm}(x_i) < \frac{\sqrt{p}}{2}$ *then* $x_1 x_2 = x_2 x_1$.

Proof.

If not, then we get a full lattice spanned by $1, x_1, x_2, x_1 x_2$. Proceed by evaluating its volume. □

Recall

We want to prove

Theorem

Write $K = \mathbb{Q}(\sqrt{d})(\sqrt{r})$, d a $\square$-free integer, $r = a + b\sqrt{d}$, $a, b \in \mathbb{Z}$ totally negative. If p is an evil prime then

$$p \leq d^2 \operatorname{Tr}(r)^2.$$

Recall

We want to prove

Theorem

Write $K = \mathbb{Q}(\sqrt{d})(\sqrt{r})$, d a $\square$-free integer, $r = a + b\sqrt{d}, a, b \in \mathbb{Z}$ totally negative. If p is an evil prime then

$$p \leq d^2 \operatorname{Tr}(r)^2.$$

Sketch of proof

- Show that we get an embedding $\mathcal{O}_K \hookrightarrow \mathrm{End}(E_1 \times E_2)$ with

$$\sqrt{d} \mapsto \left(\begin{smallmatrix} a & b \\ b^\vee & -a \end{smallmatrix}\right), \quad a \in \mathbb{Z}, b \in Hom(E_2, E_1), a^2 + bb^\vee = d.$$

  Find conditions on the image $\left(\begin{smallmatrix} x & y \\ z & w \end{smallmatrix}\right)$ of $\sqrt{r}$ as well, using that Rosati, $\left(\begin{smallmatrix} x & y \\ z & w \end{smallmatrix}\right) \mapsto \left(\begin{smallmatrix} x^\vee & z^\vee \\ y^\vee & w^\vee \end{smallmatrix}\right)$, takes $\sqrt{r}$ to $-\sqrt{r}$ and that we already know $\sqrt{r}^2$.
- Assume for simplicity that $E_1 = E_2$. Then one proceeds to show that the conditions imply that all the entries a, b, x, y, z, w are bounded in norm by a bound that depends on the field K only.
  Example: $\mathrm{Norm}(a), \mathrm{Norm}(b) \leq d$.

Sketch of proof

- Show that we get an embedding $\mathcal{O}_K \hookrightarrow \mathrm{End}(E_1 \times E_2)$ with

$$\sqrt{d} \mapsto \begin{pmatrix} a & b \\ b^\vee & -a \end{pmatrix}, \quad a \in \mathbb{Z}, b \in Hom(E_2, E_1), a^2 + bb^\vee = d.$$

  Find conditions on the image $\begin{pmatrix} x & y \\ z & w \end{pmatrix}$ of $\sqrt{r}$ as well, using that Rosati, $\begin{pmatrix} x & y \\ z & w \end{pmatrix} \mapsto \begin{pmatrix} x^\vee & z^\vee \\ y^\vee & w^\vee \end{pmatrix}$, takes $\sqrt{r}$ to $-\sqrt{r}$ and that we already know $\sqrt{r}^2$.

- Assume for simplicity that $E_1 = E_2$. Then one proceeds to show that the conditions imply that all the entries a, b, x, y, z, w are bounded in norm by a bound that depends on the field K only.
  Example: $\mathrm{Norm}(a), \mathrm{Norm}(b) \leq d$.

Sketch of proof

- Show that we get an embedding $\mathcal{O}_K \hookrightarrow \mathrm{End}(E_1 \times E_2)$ with

$$\sqrt{d} \mapsto \left(\begin{smallmatrix} a & b \\ b^\vee & -a \end{smallmatrix}\right), \quad a \in \mathbb{Z}, b \in Hom(E_2, E_1), a^2 + bb^\vee = d.$$

  Find conditions on the image $\left(\begin{smallmatrix} x & y \\ z & w \end{smallmatrix}\right)$ of $\sqrt{r}$ as well, using that Rosati, $\left(\begin{smallmatrix} x & y \\ z & w \end{smallmatrix}\right) \mapsto \left(\begin{smallmatrix} x^\vee & z^\vee \\ y^\vee & w^\vee \end{smallmatrix}\right)$, takes $\sqrt{r}$ to $-\sqrt{r}$ and that we already know $\sqrt{r}^2$.
- Assume for simplicity that $E_1 = E_2$. Then one proceeds to show that the conditions imply that all the entries a, b, x, y, z, w are bounded in norm by a bound that depends on the field K only.
  Example: $\mathrm{Norm}(a), \mathrm{Norm}(b) \leq d$.

Sketch of proof (cont'd)

- Conclude that if p is large enough, all these entries belong to a quadratic imaginary subfield K_1 of $B_{p,\infty}$.
- Conclude $K \hookrightarrow M_2(K_1)$ and so $K_1 \hookrightarrow K$, which contradicts primitivity of K.
- In the general case, $E_1 \neq E_2$, get back to the case of $E_1 = E_2$ by a suitable isogeny at the expense of introducing denominators that can be effectively bounded.

□

Sketch of proof (cont'd)

- Conclude that if p is large enough, all these entries belong to a quadratic imaginary subfield K_1 of $B_{p,\infty}$.
- Conclude $K \hookrightarrow M_2(K_1)$ and so $K_1 \hookrightarrow K$, which contradicts primitivity of K.
- In the general case, $E_1 \neq E_2$, get back to the case of $E_1 = E_2$ by a suitable isogeny at the expense of introducing denominators that can be effectively bounded.

□

Sketch of proof (cont'd)

- Conclude that if p is large enough, all these entries belong to a quadratic imaginary subfield K_1 of $B_{p,\infty}$.
- Conclude $K \hookrightarrow M_2(K_1)$ and so $K_1 \hookrightarrow K$, which contradicts primitivity of K.
- In the general case, $E_1 \neq E_2$, get back to the case of $E_1 = E_2$ by a suitable isogeny at the expense of introducing denominators that can be effectively bounded.

□

Sketch of proof (cont'd)

- Conclude that if p is large enough, all these entries belong to a quadratic imaginary subfield K_1 of $B_{p,\infty}$.
- Conclude $K \hookrightarrow M_2(K_1)$ and so $K_1 \hookrightarrow K$, which contradicts primitivity of K.
- In the general case, $E_1 \neq E_2$, get back to the case of $E_1 = E_2$ by a suitable isogeny at the expense of introducing denominators that can be effectively bounded.

□