Supersingular $\mathbb{Z}_p$ j-Invariants of CM-Elliptic Curves

Andrew Fiori

University of Calgary

Fall 2015

Goals

The goal of this talk is to very briefly summarize some recent results of mine. For the benefit of the junior members of the audience I will spend more time stating important background results than giving any actual proofs.

But first, as the background may take a while, just to give those who will already understand the background a taste, a concrete example.

Example

Let $\mathcal{O}$ be any quadratic imaginary order of discriminant $-D$ and conductor $f \in \mathbb{Z}$ with $\left(\frac{-Df^2}{71}\right) = -1$ and such that $2 \nmid f$.

Let $S_{48}(\mathcal{O}) \subset \mathbb{Z}_{71}$ (respectively $S_{66}(\mathcal{O}) \subset \mathbb{Z}_{71}$) denote the set of j-invariants congruent to 48 (respectively 66) modulo 71 for elliptic curves defined over $\mathbb{Z}_{71}$ which (after base extension) admit CM by $\mathcal{O}$.

We have the following:

- If $2 \nmid D$ then $|S_{48}(\mathcal{O})| = 0$.
- If $4||D$ then $|S_{48}(\mathcal{O})| = |S_{66}(\mathcal{O})|$.
- If $8||D$ then $|S_{66}(\mathcal{O})| = 0$.
- If $7|Df$ then $|S_{48}(\mathcal{O})| = |S_{66}(\mathcal{O})| = 0$.

Note: there exist $\mathcal{O}$ for which these sets are arbitrarily large.

Elliptic Curves over $\mathbb{C}$

Perhaps the easiest way to define an elliptic curve over $\mathbb{C}$ is to consider its complex points as a quotient of $\mathbb{C}$ by a discrete lattice. Given τ in the complex upper half plane we can consider:

$$E_\tau(\mathbb{C}) = \mathbb{C}/(\mathbb{Z} \oplus \tau\mathbb{Z})$$

It will be a complex analytic variety with a canonical Abelian group structure.

Theorem

All complex analytic elliptic curves can be constructed as above. The isomorphism class of E_τ depends only on τ module $SL_2(\mathbb{Z})$ acting by fractional linear transformations.

Unfortunately an analytic description isn't so useful to us, so we must obtain an algebraic one.

An Algebraic Description

To convert this to an algebraic description we shall use the function $j(\tau)$ from the upper half plane to $\mathbb{C}$. The function has a well known Fourier expansion:

$$j(\tau) = e^{-2\pi i\tau} + 744 + 196884e^{2\pi i\tau} + 21493760e^{4\pi i\tau} + \dots$$

Theorem

The curve E_τ is isomorphic to the (smooth projective) algebraic curve defined by:

$$y^2 = x^3 - 3j(\tau)(j(\tau) - 1728)x - 2j(\tau)(j(\tau) - 1728)^2$$

unless $j(\tau) = 0, 1728$ [a problem which can be dealt with hence we ignore]

Moreover, two elliptic curves E_{τ_1} and E_{τ_2} are isomorphic over an algebraically closed field if and only if $j(\tau_1) = j(\tau_2)$.

By the above, we may freely write $j(E_\tau)$ or $j(E)$ instead of $j(\tau)$.

Endomorphism Algebras

As elliptic curves admit algebraically defined group laws, we may consider the endomorphism algebra: $End(E)$ of E.

Theorem

If E is an elliptic curve over $\mathbb{C}$ then either:

- $End(E) = \mathbb{Z}$, *this is the general case.*
- $End(E) \simeq \mathcal{O}$, *for $\mathcal{O} \subset \mathbb{Q}(\sqrt{-D})$ an order in a quadratic imaginary field, this is the so-called CM-case.*

The CM-case will be the one we are actually interested in.

Complex Multiplication

We can understand which curves admit CM from the analytic description

Theorem

The elliptic curve $E_\tau = \mathbb{C}/(\mathbb{Z} \oplus \tau\mathbb{Z})$ has $End(E) \simeq \mathcal{O}$ if and only if

1. *$\tau \in \mathbb{Q}(\sqrt{-D})$, that is τ generates a (complex) quadratic field, and*
2. *$\mathbb{Z} + \tau\mathbb{Z} \subset \mathbb{Q}(\sqrt{-D})$ is a (projective) $\mathcal{O}$-module.*

Moreover, there is a bijective correspondence between elliptic curves over $\mathbb{C}$ for which $End(E) \simeq \mathcal{O}$ and $C\ell(\mathcal{O})$ the ideal class group of $\mathcal{O}$. (the group of invertible ideals modulo principal ideals).

We shall denote by $CM(\mathcal{O})$ this set of elliptic curves which admit complex multiplication by $\mathcal{O}$.

Some Galois Theory

If $\sigma \in Aut_{\mathbb{Q}}(\mathbb{C})$, that is σ is a $\mathbb{Q}$-algebra automorphism of $\mathbb{C}$, and if:

$$y^2 = x^3 - 3j(j-1728)x - 2j(j-1728)^2$$

defines an elliptic curve with CM by $\mathcal{O}$, then so does:

$$y^2 = x^3 - 3\sigma(j)(\sigma(j)-1728)x - 2\sigma(j)(\sigma(j)-1728)^2.$$

It follows from this that the $j(E)$ are algebraic numbers and moreover that:

$$P(X) = \prod_{E \in CM(\mathcal{O})} (X - j(E))$$

is a polynomial with coefficients in $\mathbb{Q}$.

Some Amazing Facts

- The action of $Gal(\overline{K}/K)$ on $CM(\mathcal{O})$ commutes with the action of $C\ell(\mathcal{O})$ and hence we have a map:

$$Gal(\overline{K}/K) \to C\ell(\mathcal{O}).$$

- $Gal(\overline{K}/K)$ acts transitively on $CM(\mathcal{O})$.
  Consequently:
  - $P(X)$ is irreducible over K.
  - $M = \mathbb{Q}[X]/(P(X))$ and $L = K[X]/(P(X))$ are fields.
  - L is Galois over K and the map $Gal(L/K) \to C\ell(\mathcal{O})$ is an isomorphism.
  - In particular the Galois group of L/K is Abelian.
- When $\mathcal{O}$ is stable under $Gal(K/\mathbb{Q})$, then:

$$Gal(L/\mathbb{Q}) = Gal(L/K) \rtimes Gal(K/\mathbb{Q}).$$

- The polynomial $P(X)$ is actually in $\mathbb{Z}[X]$.

Elliptic Curves in Characteristic p

One clever way to study polynomials and their Galois groups is to reduce modulo p. We can then exploit the fact that Galois theory for finite fields is quite simple to study subgroups of the original Galois group. To do this in our context we will need to know a little bit about Elliptic curves in characteristic p.

We can't (easily) define an elliptic curve in characteristic p as the quotients of a ring like we did for elliptic curves over $\mathbb{C}$.

However, we can still fairly easily define the variety by writing down equations such as:

$$y^2 = x^3 - 3j(j-1728)x - 2j(j-1728)^2$$

and vary j over elements of $\overline{\mathbb{F}}_p$ [again ignoring difficulty when $j = 0, 1728$].

Endomorphisms in Characteristic p

Such curves end up having canonical Abelian group structures, and we can still study their endomorphism rings.

Theorem

If E is an elliptic curve over $\overline{\mathbb{F}}_p$ then $End(E)$ is one of:

- $\mathbb{Z}$.
- *An order $\mathcal{O} \subset \mathbb{Q}(\sqrt{-D})$ where $-D$ is a square modulo p.*
- *An order in a quaternion algebra (ramified only at p and $\mathbb{R}$). We call this new case supersingular.*

Notice that the CM-case is now slightly more restrictive, and there is an additional supersingular case. In characteristic p it will be this supersingular case we are interested in.

Reducing modulo primes

As $P(X) \in \mathbb{Z}[X]$ its roots, $j(\tau)$, are algebraic integers, it makes sense to consider there reduction modulo p, (more accurately modulo $\mathfrak{p}|p$ for $\mathfrak{p}$ a prime ideal of the ring of integers of L).

Reduction can also be carried out on the equation defining the curve:

$$y^2 = x^3 - 3j(\tau)(j(\tau) - 1728)x - 2j(\tau)(j(\tau) - 1728)^2 \pmod{\mathfrak{p}}$$

resulting in the equation for an elliptic curve $\overline{E}$ over $\overline{\mathbb{F}}_p$.
We can also reduce the equations defining the endomorphisms, and thus reductions yields a map from the set of elliptic curves over $\mathbb{C}$ with endomorphism ring $\mathcal{O}$ to the set of elliptic curves over $\overline{\mathbb{F}}_p$ where $\mathcal{O}$ is a subring of the endomorphism ring.

What Can Happen When we Reduce?

There are three main cases:

- $p|f^2D$ (where f is the conductor of $\mathcal{O}$),
- $-Df^2$ is a square modulo p, or
- $-Df^2$ is not a square modulo p.

We will be most interested in the last case, that is when $-Df^2$ is not a square modulo p. In this case we find:

- The endomorphism ring of $\overline{E}$ is larger than $\mathbb{Z}$, but can't be $\mathcal{O}$, hence $\overline{E}$ must be 'supersingular' at p.
- Algebraic number theory (plus class field theory) lets us show that $P(X)$ factors as a product of linear/quadratic terms over $\mathbb{Z}_p$ (and consequently $\mathbb{F}_p$).

Key point:
In the case we care about, the reductions of the j-invariants will all be supersingular values in $\mathbb{F}_{p^2}$.

What is known about the image?

Many things are known about these supersingular reductions. For example:

If we fix p, and consider values of $-D$ and f with $\left(\frac{-Df^2}{p}\right) = -1$ then:

- For D sufficiently large the set $j(CM(\mathcal{O}))$ surjects onto the set of supersingular values (Jetchev-Kane).
- The values $j(\tau)$ are equidistributed (Cornut-Vatsal, Jetchev-Kane).

Note that this equidistribution requires varying both D and the order $\mathcal{O} \subset \mathbb{Q}(\sqrt{-D})$ but still holds when we impose certain types of congruence conditions on D and f.

Some Computations:

We wanted to compute lots of examples for some reason, we were interested in factoring the polynomial $P(X)$ over $\mathbb{Z}_p$ at supersingular primes and studying the factors (which would be quadratic and linear).
I computed too many examples to actually look at them all, so I computed some summary statistics in which I grouped factors by their reductions modulo p.
Given that the roots of these polynomials are supposedly equidistributed modulo p we figured the factors we obtained would be too, and so the summary data should be pretty boring.

The data in the next few slides gives the total frequency of each factor (grouped modulo p) across all maximal orders in all imaginary quadratic fields with odd class numbers between 1 and 39 with discriminants between 1 and 10000000 for which $-D$ is not a square modulo p.

This table is for $p = 23$, there are only 3 supersingular values.

Polynomial	Frequency	Observations
x	459	
$x + 4$	1	only 1??
$x + 20$	223	
x^2	2700	
$(x + 4)^2$	9484	
$(x + 20)^2$	4486	

Galois theory/Chebotarev density explains why there are way more quadratics than linear terms.

Theorem:
That 1 is a 1, even if I consider all maximal orders in all quadratic imaginary fields with odd class number where $\left(\frac{-D}{23}\right) = -1$. (the actual theorems are far more general).

This is $p = 59$.

Polynomial	Frequency	observations
x	151	j=0
$x + 11$	135	
$x + 12$	140	
$x + 31$	140	
$x + 42$	73	j=1728
$x + 44$	0	missing??
x^2	994	j=0
$(x + 11)^2$	3252	
$(x + 12)^2$	3168	
$(x + 31)^2$	3228	
$(x + 42)^2$	1590	j=1728
$(x + 44)^2$	3264	

Note that the equidistribution results actually tell us we should reweight the 0 and 1728 values based on the size of the automorphism groups.

This is $p = 71$.

Polynomial	Frequency	observations
x	199	j=0
$x+5$	188	
$x+23$	1	j=8000
$x+30$	171	
$x+31$	0	missing??
$x+47$	88	j=1728
$x+54$	0	missing??
x^2	742	j=0
$(x+5)^2$	2618	
$(x+23)^2$	2832	
$(x+30)^2$	2650	
$(x+31)^2$	2846	
$(x+47)^2$	1308	j=1728
$(x+54)^2$	2762	

Why is $j = 8000$ special? This is actually the key to the whole thing, and the concrete example from the start should ruin the mystery.

More hints about what is happening

Firstly, I should point out that 8000 is the j-invariant for the ring of integers of $\mathbb{Q}(\sqrt{-2})$, which explains why it has to appear at least once, though not why it never appears otherwise.

For more fun facts I should give a much bigger 'hint' by pointing out that:

$$x + 44 = x - 16581375 \text{ module } 59$$
$$x + 31 = x - 54000 \text{ modulo } 71$$
$$x + 54 = x - 287496 \text{ modulo } 71$$

A few of you might recognize the numbers 16581375, 54000, and 287496 as j-invariants of certain famous CM elliptic curves.

Theorem (refined):
For all $p = 3 \pmod 4$ the 8000 always gets a one, the others above always get 0's, even if I consider all maximal orders in all quadratic imaginary fields with odd class number where $\left(\frac{-D}{p}\right) = -1$.

Theorem: $p = 7 \pmod 8$ then this pattern happens

$\mathcal{O}$ with $h_{\mathcal{O}} < 40$ and $\left(\frac{-Df^2}{71}\right) = -1$ for $p = 71$. (Note: $\left(\frac{-71}{7}\right) = -1$).

	All	$2 \nmid D$ $2 \nmid f$	$2 \nmid D$ $2 \| f$	$2 \nmid D$ $4 \| f$	$2 \nmid D$ $8 \mid f$	$4 \| D$ $2 \nmid f$	$4 \| D$ $2 \| f$	$4 \| D$ $4 \| f$	$4 \| D$ $8 \mid f$	$8 \| D$ $2 \nmid f$	$8 \| D$ $2 \| f$	$8 \| D$ $4 \| f$	$8 \| D$ $8 \mid f$	$7 \mid Df$	$7 \nmid Df$
x	1109	806	-	-	23	158	-	17	7	-	73	16	9	-	1109
$x+5$	1123	817	-	-	25	152	-	16	9	-	74	22	8	-	1123
$x+23$	941	-	173	82	19	152	75	17	6	314	73	21	9	-	941
$x+30$	1126	811	-	-	30	161	-	11	9	-	74	23	7	-	1126
$x+31$	967	-	176	94	32	158	77	11	9	303	75	23	9	-	967
$x+47$	1027	408	86	48	20	143	39	17	10	155	74	22	5	-	1027
$x+54$	934	-	169	86	23	161	66	17	10	301	79	15	7	-	934
x^2	2981	1572	432	101	22	298	90	12	8	378	47	19	2	467	2514
$(x+5)^2$	10258	5675	1293	310	81	1078	267	55	32	1164	207	72	24	1447	8811
$(x+23)^2$	10375	6106	1194	278	74	1086	229	60	29	1009	219	63	28	1427	8948
$(x+30)^2$	10214	5661	1292	304	67	1068	271	60	27	1159	208	69	28	1418	8796
$(x+31)^2$	10283	6052	1213	251	78	1062	236	61	32	1001	207	73	17	1414	8869
$(x+47)^2$	4833	2787	598	134	32	499	118	26	17	509	78	28	7	721	4112
$(x+54)^2$	10255	6042	1187	258	70	1065	235	54	31	1001	218	71	23	1450	8805

Theorem: $p = 3 \pmod 8$ then this pattern happens

All $\mathcal{O}$ with $h_{\mathcal{O}} < 40$ and $\left(\frac{-Df^2}{59}\right) = -1$ for $p = 59$.

	All All	$2 \nmid D$ $2 \nmid f$	$2 \nmid D$ $2 \| f$	$2 \nmid D$ $4 \| f$	$2 \nmid D$ $8 \mid f$	$4 \| D$ $2 \nmid f$	$4 \| D$ $2 \| f$	$4 \| D$ $4 \| f$	$4 \| D$ $8 \mid f$	$8 \| D$ $2 \nmid f$	$8 \| D$ $2 \| f$	$8 \| D$ $4 \| f$	$8 \| D$ $8 \mid f$
x	1245	896	-	92	-	172	85	-	-	-	-	-	-
$x+11$	1241	890	-	98	-	173	80	-	-	-	-	-	-
$x+12$	1236	890	-	97	-	167	82	-	-	-	-	-	-
$x+31$	1224	870	-	91	-	172	91	-	-	-	-	-	-
$x+42$	1146	440	285	40	-	336	45	-	-	-	-	-	-
$x+44$	1060	-	549	-	-	511	-	-	-	-	-	-	-
$(x+11)^2$	12375	6855	1574	325	132	1269	299	85	44	1389	297	92	14
$(x+12)^2$	12241	6818	1537	319	125	1229	293	84	53	1371	306	93	13
$(x+31)^2$	12274	6844	1544	324	125	1250	282	83	57	1381	292	83	17
$(x+42)^2$	5910	3429	632	160	63	511	144	39	26	701	145	52	8
$(x+44)^2$	12360	7250	1264	381	143	1066	329	80	46	1399	300	87	15
x^2	3692	1983	512	77	38	352	72	26	20	474	100	33	5

$p = 1 \pmod 4$

All $\mathcal{O}$ with $h_{\mathcal{O}} < 40$ and $\left(\frac{-Df^2}{41}\right) = -1$ for $p = 41$.

	All	$2 \nmid D$ $2 \nmid f$	$2 \nmid D$ $2 \| f$	$2 \nmid D$ $4 \| f$	$2 \nmid D$ $8 \mid f$	$4 \| D$ $2 \nmid f$	$4 \| D$ $2 \| f$	$4 \| D$ $4 \| f$	$4 \| D$ $8 \mid f$	$8 \| D$ $2 \nmid f$	$8 \| D$ $2 \| f$	$8 \| D$ $4 \| f$	$8 \| D$ $8 \mid f$
x	1488	1055	222	-	-	-	-	-	-	211	-	-	-
$x+9$	1495	1068	220	-	-	-	-	-	-	207	-	-	-
$x+13$	1491	1055	229	-	-	-	-	-	-	207	-	-	-
$x+38$	1499	1065	223	-	-	-	-	-	-	211	-	-	-
x^2	5583	3036	665	184	59	675	146	37	10	560	146	45	20
$(x+9)^2$	18184	10102	2215	557	191	2014	454	117	40	1877	434	135	48
$(x+13)^2$	18218	10107	2199	582	185	2001	444	123	40	1906	443	132	56
$(x+38)^2$	18173	10080	2205	583	185	2015	432	131	46	1871	437	128	60

"Theorem" /Hint at Proof

The patterns you see above generalize fully based only on the congruence of p modulo 8.

"Theorem" /Hint at Proof

The patterns you see above generalize fully based only on the congruence of p modulo 8.

An empty column is always explained by genus theory, "The totally real subfield of the genus field of the ring class field associated to $\mathcal{O}$ contains a quadratic sub-extension in which p is inert." One can describe the conditions explicitly (ie. interpolate exactly from tables, note for odd $q|Df$ the condition $\left(\frac{-p}{q}\right) = -1$ implies this).

"Theorem" /Hint at Proof

The patterns you see above generalize fully based only on the congruence of p modulo 8.

An empty column is always explained by genus theory, "The totally real subfield of the genus field of the ring class field associated to $\mathcal{O}$ contains a quadratic sub-extension in which p is inert." One can describe the conditions explicitly (ie. interpolate exactly from tables, note for odd $q|Df$ the condition $\left(\frac{-p}{q}\right) = -1$ implies this).

The sets which appear/don't appear when $p = 3$ modulo 4 are based on the fact that some supersingular elliptic curves admit CM (optimally) only by $\mathbb{Z}[\sqrt{-p}]$ while others admit CM by $\mathbb{Z}[\frac{1+\sqrt{-p}}{2}]$ (only $j = 1728$ does both optimally).

"Theorem" /Hint at Proof

The patterns you see above generalize fully based only on the congruence of p modulo 8.

An empty column is always explained by genus theory, "The totally real subfield of the genus field of the ring class field associated to $\mathcal{O}$ contains a quadratic sub-extension in which p is inert." One can describe the conditions explicitly (ie. interpolate exactly from tables, note for odd $q|Df$ the condition $\left(\frac{-p}{q}\right) = -1$ implies this).

The sets which appear/don't appear when $p = 3$ modulo 4 are based on the fact that some supersingular elliptic curves admit CM (optimally) only by $\mathbb{Z}[\sqrt{-p}]$ while others admit CM by $\mathbb{Z}[\frac{1+\sqrt{-p}}{2}]$ (only $j = 1728$ does both optimally).

The pairing between the two sets when $p = 3$ modulo 4 is based on the existence of unique $\mathbb{F}_p$ rational 2-isogenies.

"Theorem" /Hint at Proof

The patterns you see above generalize fully based only on the congruence of p modulo 8.

An empty column is always explained by genus theory, "The totally real subfield of the genus field of the ring class field associated to $\mathcal{O}$ contains a quadratic sub-extension in which p is inert." One can describe the conditions explicitly (ie. interpolate exactly from tables, note for odd $q|Df$ the condition $\left(\frac{-p}{q}\right) = -1$ implies this).

The sets which appear/don't appear when $p = 3$ modulo 4 are based on the fact that some supersingular elliptic curves admit CM (optimally) only by $\mathbb{Z}[\sqrt{-p}]$ while others admit CM by $\mathbb{Z}[\frac{1+\sqrt{-p}}{2}]$ (only $j = 1728$ does both optimally).

The pairing between the two sets when $p = 3$ modulo 4 is based on the existence of unique $\mathbb{F}_p$ rational 2-isogenies.

The pairing between j-invariants when $p = 1$ modulo 4 is based on the existence of a 2-isogeny between curves admitting CM by $\mathbb{Z}[\sqrt{-p}]$.

Future Work

At this point I can explain and prove all the paterns I have seen, though there are a few questions hinted at by the proof, it doesn't immediately seem like there is much left to do...

That said, the original goal of computing this data had nothing to do with looking at phenomenon over $\mathbb{Z}_p$ vs $\mathbb{Z}_{p^2}$. You may notice I have computed thousands of examples over $\mathbb{Z}_{p^2}$, and though the modulo p behaviour of j-invariants is equidistributed, there may be other more subtle things in the data to look at...
I just don't know what they are, if someone has good ideas for what to do with the data, I am interested to hear them.

Even if it is just something unrelated you want to do with the $P_{\mathcal{O}}(X)$ for all rings of low class number.

The End.

Thank you.