Distribution of J-Invariants of CM-Elliptic Curves Modulo p

Andrew Fiori

Queen's University

Fall 2014

Goals

The main goal of this talk is to explain some surprising and somewhat mysterious results that came out of some computations I was doing. The goal isn't so much to show you the solution to the mystery as it is tell you the story behind it.

In any case like many mysteries, it wouldn't be all that interesting without some backstory on the characters. So first we will go through a bit of background.

- Some of the general theory of elliptic curves with complex multiplication and the role they play in Galois theory.
- The reduction of CM-elliptic curves modulo a prime p.
- Known properties of the distribution of j-invariants modulo p.

Note: This comes out of joint work with Eyal Goren at McGill.

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

Our version of the algebraic story begins with a complex analytic function $j(\tau)$ from the upper half plane to $\mathbb{C}$
given by the Fourier expansion:

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

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

Given an elliptic curve, its points are an abelian group, and as such we have that:

$$End(E) = Hom(E, E)$$

has the canonical structure of a $\mathbb{Z}$-algebra.

Theorem

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

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

We will be interested in the CM or Complex Multiplication case.

In order to avoid technical details in a colloquium talk, it is traditional to assume $\mathcal{O}$ is a maximal order, and claim "things work similarly in the general case". I will not break this tradition, though have generally stated results in such a way to handle the non-maximal case.

Complex Multiplication

We will need to know when an elliptic curve ends up with these extra endomorphisms, this is easiest to understand in the analytic description.

Theorem

The elliptic curve $E_\tau = \mathbb{C}/(\mathbb{Z} \oplus \tau\mathbb{Z})$ has $End(E) = \mathcal{O}$ 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 $\mathbb{C}$ with $End(E) = \mathcal{O}$ and $C\ell(\mathcal{O})$ the ideal class group of $\mathcal{O}$. (the group of invertible ideals modulo principal ideals).

As such, we could identify $C\ell(\mathcal{O})$ with the set of CM-elliptic curves, however, this is (secretly) misleading, so we instead denote by $CM(\mathcal{O})$ this set of elliptic curves with complex multiplication by $\mathcal{O}$.

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:

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

As the ideal class group $C\ell(\mathcal{O})$ is finite, and $C\ell(\mathcal{O})$ acts transitively on $CM(\mathcal{O})$, the set $CM(\mathcal{O})$ is also finite. It follows from the above that the $j(E)$ are algebraic numbers.
Thus by Galois theory:

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

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 maximal (or more generally 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 $\mathbb{Z}[X]$.

Some Remarks

The proofs of the previous statements are actually far less trivial than might at first be suggested by the fact that we appear to be naturally labeling the roots of $P(X)$ by elements of a group.

The results of the previous slide are part of the main theorem of complex multiplication and describes (most of [when we allow non-maximal orders]) explicit class field theory (abelian Galois extensions) for quadratic imaginary extensions [the "most of" can be dealt with, but we won't do that here].

It can be thought of as largely equivalent to the Kronecker-Weber Theorem which describes all the abelian extensions of $\mathbb{Q}$ as being generated by $e^{2\pi i z}$ for $z \in \mathbb{Q}$.

In our case the abelian extensions are generated by $j(\tau)$ for $\tau \in \mathbb{Q}(\sqrt{-D}) \setminus \mathbb{Q}$, the function $j(\tau)$ is very much a transcendental function. Generalizing this result further is "Kronecker's Jugendtraum" and Hilberts 12th problem.

Elliptic Curves in Characteristic p

One clever way to study Galois groups is to reduce the polynomials 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. (This trick is an important part of the proofs of those previous results).

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 are algebraic integers, and so the roots, $j(\tau)$, can be reduced modulo p, (or 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 $\overline{\mathbb{F}}_p$.

As the reduction can be done to every equation in sight, including those defining endomorphisms we obtain a map from the set $CM(\mathcal{O})(\mathbb{C})$ of elliptic curves over $\mathbb{C}$ with endomorphism ring $\mathcal{O}$ to the set $CM(\mathcal{O})(\overline{\mathbb{F}}_p)$ of elliptic curves over $\overline{\mathbb{F}}_p$ where $\mathcal{O}$ is a subring of the endomorphism ring.

(this map is Galois equivariant for the map from the decomposition group $D(\mathfrak{p}|p) \subset Gal(L/\mathbb{Q})$ to $Gal(\mathbb{F}_{p^f}/\mathbb{F}_p)$).

Remark

We really should note that the proof that $P(X) \in \mathbb{Z}[X]$ is carried out in the opposite direction of what we do here. Rather, the proof first establishes the fact that we can obtain models for the curves with integer coefficients, and uses this to show that the j invariants are integral and hence that $P(X) \in \mathbb{Z}[X]$.

We should also mention, the choice of prime $\mathfrak{p}|p$ is not canonical, thus neither is the decomposition group, nor the association between roots of $P(X)$ in L and roots of $P(X)$ over $\overline{\mathbb{F}}_p$.

What Happens When we Reduce?

There are three main cases:

- $p|D$ (or some other conditions relative to the conductor of $\mathcal{O}$),
- $-D$ is a square modulo p, or
- $-D$ is not a square modulo p.

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

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

  This agrees with the fact that supersingular curves all have $j(E) \in \mathbb{F}_{p^2}$.

Key point:
We thus have a map from $CM(\mathcal{O})$ to supersingular values in $\mathbb{F}_{p^2}$.

We are interested in studying the image of this map.

What is known about the image?

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

- If we fix p, and consider values of $-D$ which are not squares modulo p.
  - 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 $\mathcal{O} \subset \mathbb{Q}(\sqrt{-D})$.
- Gross-Zagier gave a formula for computing the factorization of the constant term $P(0)$.
  They have an algebraic proof which focuses on the case $\mathcal{O}$ a maximal order with odd class number.

(What we are actually looking to obtain is a more precise understanding of the roots of $P(X)$.)

That is what we know about the characters, what did we do with them?

We wanted to compute lots of examples, the setting of our computations:

- Because it is easier, and this is the case Gross-Zagier dealt with we consider only the case $\mathcal{O}$ the maximal order.
- Further, Gross-Zagier had made the assumption that $|C\ell(\mathcal{O})|$ was odd, so we looked at the data separately between the two cases.
- Thirdly, as we were interested in the valuations of the roots, we factor the polynomials over $\mathbb{Z}_p$ before doing the reduction. This naturally groups the terms into quadratic and linear factors. We don't bother to check if the quadratics factor further after reduction.
- In the end I computed too many examples to look at them all individually, so we collected some statistics.

What did we expect to see?

Given that the roots of these polynomials are supposedly equidistributed modulo p we figured the factors we obtained would be too.

(what we guessed was slightly more refined than this, but you will see the obvious corrections on the next few slides)

Strictly speaking our approach to computing them means they don't have to be (the factoring over $\mathbb{Z}_p$ rather than $\mathbb{F}_p$) but we had no reason to expect it to matter.

Now the mystery...

This table gives the total frequency of each factor (expressed modulo 23) across 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 23.

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

Comments on the obvious questions:

- Recall: The factors were irreducible over $\mathbb{Z}_p$ before we reduced modulo p.
- Galois theory explains why there are way more quadratics than linear terms.
- What we had expected was equidistribution of possible linear (respectively possible quadratic) terms. This is clearly not the case, the next slide explains part of this.

Maybe more data will shed some light. This is as above, except $p = 59$.

Polynomial	Frequency	
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	

- It is natural to expect the pesky 0 and 1728 values to need to be reweighted based on the size of the automorphism groups. (The referenced equidistribution results actually do this).
- Oddly, this doesn't happen for the linear $j = 0$ term. (a mystery)
- And what about the missing linear term? (another mystery)

Maybe more data will shed some light. This is as above, except $p = 71$.

Polynomial	Frequency	
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 $j = 8000$? Because we can look at our data and check where the 1 came from (this explains the previous 1 also).
- But what is the pattern with terms that are missing?

Maybe more data will shed some light. This table is as above, except $p = 107$.

Polynomial	Frequency	
x	140	j=0
$x+13$	135	
$x+26$	137	
$x+35$	0	missing??
$x+60$	142	
$x+91$	74	j=1728
x^2	452	$j=0$
$(x+13)^2$	1698	
$(x+26)^2$	1718	
$(x+35)^2$	1786	
$(x+60)^2$	1628	
$(x+91)^2$	820	j=1728
$x^2+66x+58$	3580	
$x^2+82x+30$	3610	

- Note that 8000 is not supersingular at $p = 107$ or $p = 59$, and there are no 1's in either case.

Questions and Observations?

- It is worth noticing that we have almost perfect equidistribution of roots, despite everything going wrong with the factors.
- Mystery 1: What is the pattern on the missing terms? They can't all come from a single congruence as there are 2 modulo 71. Hint: the "pattern" is by no means obvious, but based on what happens with 8000, you might be able to guess at something.
- Mystery 2: Why does $x + 8000$ factor only ever appear once?

  Fact: if there is a 1 in our data it occurs if and only if the factor is congruent to $x + 8000$ modulo p (primes up to 1000 odd class numbers 1-39).
- Mystery 3: Why are my examples all from $p = 11 \pmod{12}$?

  This I can answer, because these are the ones where both 0 and 1728 appear and so I like them more.

  (there are actually missing values in (virtually) all examples $p = 3 \pmod{4}$.)

Answers, or rather Hints

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 the next question, I should give a much bigger 'hint' by pointing out that:

$$\begin{aligned}
&x + 44 = x - 16581375 \text{ module } 59\\
&x + 31 = x - 54000 \text{ modulo } 71\\
&x + 54 = x - 287496 \text{ modulo } 71\\
&x + 35 = x - 54000 \text{ modulo } 107
\end{aligned}$$

A few of you might recognize the numbers 16581375, 54000, and 287496 as j-invariants of certain non-maximal orders where 2 divides the conductor. Note that the above factors will all be missing any time they could have appeared.

In order to better understand what is happening, we should maybe look at the even class number case for comparison.

As before, except even class numbers between 1 and 39 all for $p = 71$.

Polynomial	Frequency	
x	531	j=0
$x + 5$	557	
$x + 23$	367	j=8000
$x + 30$	587	
$x + 31$	363	j=54000
$x + 47$	447	j=1728
$x + 54$	364	j=287496
x^2	3012	j=0
$(x + 5)^2$	10432	
$(x + 23)^2$	10614	
$(x + 30)^2$	10342	
$(x + 31)^2$	10508	
$(x + 47)^2$	4974	j=1728
$(x + 54)^2$	10570	

Nothing is missing, but the terms that were before missing are still systemically under-represented.

So what is my "explanation"?

Conjectural “Explanation”

At this point I would like to suggest my prime suspect in the mystery. I blame that pesky number 2.

In order to explain the ‘missingness’ we need to consider the ramification of 2 in our order. Why would I think such a thing?

- Quadratic imaginary fields with odd class number are never ramified at 2 unless it is $\mathbb{Q}(\sqrt{-2})$ or $\mathbb{Q}(\sqrt{-1})$.
- Quadratic imaginary fields with even class number are ramified at 2 about a quarter of the time. (if you order by class number like we are)
- The three other rings we needed to find missing values all had conductors 2.

What is great about this conjecture is we can check it by only checking the orders not ramified at 2.

This table considers all class numbers between 1 and 39 but only orders for which 2 does not ramify in $\mathbb{Q}(\sqrt{-D})$ (ie $D = 3 \pmod 4$). This is all for $p = 71$.

Polynomial	Frequency	
x	605	j=0
$x+5$	627	
$x+23$	0	j=8000
$x+30$	630	
$x+31$	0	j=54000
$x+47$	311	j=1728
$x+54$	0	j=287496
x^2	2650	j=0
$(x+5)^2$	9422	
$(x+23)^2$	10066	
$(x+30)^2$	9370	
$(x+31)^2$	10000	
$(x+47)^2$	4630	j=1728
$(x+54)^2$	9968	

So our vague conjecture, as vaguely stated, is right!

Other Questions?

This whole buisness really just raises further questions.

- What is a precise formulation of the conjecture?
  Concretely we are saying that the ramification at 2 influences the possible j invariants of elliptic curves with CM over $\mathbb{Z}_p$ (but somehow not over its unramified extension, which is also mysterious).

- What is the pattern underlying the values which do not appear? Is there a systematic description of these?

  Fact: The rational j-invariants is a red herring, there are eventually missing values that don't come from these.

- Is there a 'good' number theoretic explanation?

  It is possible that the explanation will turn out to be 'obvious' or rather 'well-known' in hindsight.

My original plan was to fade out now and leave you with a good mystery, which I will still do if I am now out of time

But if I still have time... I would like to make things a little more mysterious

So what is the natural next question to ask?

This table considers all class numbers between 1 and 39 but only orders for which 2 does ramify in $\mathbb{Q}(\sqrt{-D})$ (ie $D \neq 3 \pmod 4$). This is all for $p = 71$.

Polynomial	Frequency	
x	125	j=0
$x + 5$	118	
$x + 23$	368	j=8000
$x + 30$	128	
$x + 31$	367	j=54000
$x + 47$	254	j=1728
$x + 54$	364	j=287496
x^2	1104	j=0
$(x + 5)^2$	3628	
$(x + 23)^2$	3388	
$(x + 30)^2$	3622	
$(x + 31)^2$	3354	
$(x + 47)^2$	1652	j=1728
$(x + 54)^2$	3364	

- The ones which do have 2 ramify have an over-representation of the terms which didn't appear before.

As above, except 2 wildly ramifies in $\mathbb{Q}(\sqrt{-D})$ (ie $D = 2 \pmod 4$). This is all for $p = 71$.

Polynomial	Frequency	
x	0	j=0
$x+5$	0	
$x+23$	250	j=8000
$x+30$	0	
$x+31$	238	j=54000
$x+47$	123	j=1728
$x+54$	236	j=287496
x^2	308	j=0
$(x+5)^2$	946	
$(x+23)^2$	822	
$(x+30)^2$	946	
$(x+31)^2$	823	
$(x+47)^2$	415	j=1728
$(x+54)^2$	825	

- So wild is the opposite of unramified...
- Except for $j = 1728$, which appears for both.

As above, except 2 tamely ramifies in $\mathbb{Q}(\sqrt{-D})$ (ie $D = 1 \pmod 4$)). This is all for $p = 71$.

Polynomial	Frequency	
x	125	j=0
$x+5$	118	
$x+23$	118	j=8000
$x+30$	128	
$x+31$	125	j=54000
$x+47$	101	j=1728
$x+54$	128	j=287496
x^2	244	j=0
$(x+5)^2$	868	
$(x+23)^2$	868	
$(x+30)^2$	865	
$(x+31)^2$	854	
$(x+47)^2$	411	j=1728
$(x+54)^2$	857	

- um... in the data... the linear terms do actually come in pairs... and this happens at other primes... but not all of them...
- Quadratics being equal is actually a coincidence.

As above, except for which 7 ramifies in $\mathbb{Q}(\sqrt{-D})$ (ie D is a multiple of 7). This is all for $p = 71$.

Polynomial	Frequency	
x	0	j=0
$x + 5$	0	
$x + 23$	0	j=8000
$x + 30$	0	
$x + 31$	0	j=54000
$x + 47$	0	j=1728
$x + 54$	0	j=287496
x^2	258	j=0
$(x + 5)^2$	807	
$(x + 23)^2$	804	
$(x + 30)^2$	806	
$(x + 31)^2$	798	
$(x + 47)^2$	395	j=1728
$(x + 54)^2$	816	

- So ramification at other primes can just completely prevent any linear terms from appearing.

All for which 5 ramifies in $\mathbb{Q}(\sqrt{-D})$ (ie D is a multiple of 5). This is all for $p = 71$.

Polynomial	Frequency	
x	197	j=0
$x+5$	200	
$x+23$	97	j=8000
$x+30$	216	
$x+31$	93	j=54000
$x+47$	146	j=1728
$x+54$	101	j=287496
x^2	242	j=0
$(x+5)^2$	968	
$(x+23)^2$	1035	
$(x+30)^2$	944	
$(x+31)^2$	1025	
$(x+47)^2$	445	j=1728
$(x+54)^2$	1009	

All for which 5 ramifies in $\mathbb{Q}(\sqrt{-D})$ (ie D is a multiple of 5). This is all for $p = 73$.

Polynomial	Frequency	
$x+17$	0	
$x+64$	0	
$(x+17)^2$	1030	
$(x+64)^2$	1039	
$x^2+57*x+8$	2085	
$x^2+68*x+9$	2122	

My second plan was to end things here, because I don't really want to ruin a good mystery

But there are two more slides if you want to see a hint of how things unravel.

Conjecture/Theorem

Fix $-D$, squarefree, which is not a square modulo p. There are no elliptic curves over $\mathbb{Z}_p$ with CM by maximal order of $\mathbb{Q}(\sqrt{-D})$ if either of the following occur:

- if $p = 3 \pmod 8$ and $D = 0 \pmod 2$
- there is an odd prime factor q of D with $\left(\frac{-p}{q}\right) = -1$

Otherwise there is at least one.

This is stated as a conjecture because I don't have a reference, nor have I checked the details of the proof (though it isn't all that hard to prove, so presumably it is known).

(Note that we can't just use the Kronecker symbol and drop the odd requirement in the second condition even though that subsume the first condition. This is because the $p = 5 \pmod 8$ case is more subtle and depends on $D \pmod 8$, the second condition ends up handling these cases (unless I screwed up in my quick check and there are no counterexamples in my data somehow).)

Conjectures for impossible reductions of j-invariants of elliptic curves over $\mathbb{Z}_p$ with CM by maximal order of $\mathbb{Q}(\sqrt{-D})$ based on ramification at 2.

- If $p = 3 \pmod 4$ and 2 is unramified, then there will be no elliptic curves whose j-invariants are the same modulo p as those coming from $\mathbb{Q}(\sqrt{-p})$ (except $j = 1728$).

  If $p = 3 \pmod 8$ this is $(n-2)/4$ missed curves.

  If $p = 7 \pmod 8$ this is $(n-1)/2$ missed curves.
- If $p = 7 \pmod 8$ and 2 divides D then all elliptic curves have j-invariants the same as those coming from $\mathbb{Q}(\sqrt{-p})$
- If $p = 7 \pmod 8$ and 2 is tamely ramified then there is a matching between curves (one from $\mathbb{Q}(\sqrt{-p})$ and one not).
- If $p = 1 \pmod 4$ and 2 divides D then there is a matching between curves.

  Note: If $p = 1 \pmod 4$ then j-invariants of $\mathbb{Q}(\sqrt{-p})$ take on all values.

Parts of the above should follow from, or at a minimum, be suggested by the work of Deuring, Ibukiyama, and Dorman. Though the details of why some of the above would be true is still mysterious.

The Actual End.

Thank you.