Supersingular reduction of elliptic curves

introductory lecture at

VaNTAGe series 10

26 October 2021

Noam D. Elkies
Harvard University

Overview

1. **Preliminaries: elliptic curves and** $\mathrm{Hom}(E, E')$

2. **Primes of supersingular reduction**

3. **Further variations**

1. Preliminaries: elliptic curves and $\mathrm{Hom}(E, E')$

Elliptic curve E over a field k: projective curve of genus 1 with a rational point O.

Riemann-Roch gives functions $x, y \in k(E)$ regular except for double and triple poles at O. They generate $k(E)$ and satisfy (extended) Weierstrass equation

$$y^2 + a_1 xy + a_3 y = x^3 + a_2 x^2 + a_4 x + a_6 = 0$$

[sic: a_i, x, y of weight $i, 2, 3$] for some $a_i \in k$. Conversely, given a_i with $\Delta = \Delta(a_1, a_2, a_3, a_4, a_6)$ we get an elliptic curve.

Different choices of x, y give various a_i but same *j-invariant* $j = c_4^3/\Delta$, where $c_4 = (a_1^2 + 4a_2)^2 - 24(a_1 a_3 + 2a_4)$. Conversely if $j(E) = j(E')$ then $E \cong E'$ over $\bar{k}$. [“The j-line is a coarse moduli space for elliptic curves.”]

If $6 \neq 0$ in k we can assume $a_1 = a_2 = a_3 = 0$, and then $j = 4 \cdot 12^3 a_4^3/(4a_4^3 + 27a_6^2)$. [For future use: $a_4 = 0 \Leftrightarrow j = 0$, and $a_6 = 0 \Leftrightarrow j = 1728$.]

1. Preliminaries: elliptic curves and $\mathrm{Hom}(E, E')$

Elliptic curve E over a field k: projective curve of genus 1 with a rational point O.

Riemann-Roch gives functions $x, y \in k(E)$ regular except for double and triple poles at O. They generate $k(E)$ and satisfy (extended) Weierstrass equation

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6 = 0$$

[sic: a_i, x, y of weight $i, 2, 3$] for some $a_i \in k$. Conversely, given a_i with $\Delta = \Delta(a_1, a_2, a_3, a_4, a_6)$ we get an elliptic curve.

Different choices of x, y give various a_i but same j-*invariant* $j = c_4^3/\Delta$, where $c_4 = (a_1^2+4a_2)^2-24(a_1a_3+2a_4)$. Conversely if $j(E) = j(E')$ then $E \cong E'$ <u>over $\bar{k}$</u>. ["The j-line is a coarse moduli space for elliptic curves."]

If $6 \neq 0$ in k we can assume $a_1 = a_2 = a_3 = 0$, and then $j = 4 \cdot 12^3 a_4^3/(4a_4^3 + 27a_6^2)$. [For future use: $a_4 = 0 \Leftrightarrow j = 0$, and $a_6 = 0 \Leftrightarrow j = 1728$.]

1. Preliminaries: elliptic curves and $\mathrm{Hom}(E, E')$

Elliptic curve E over a field k: projective curve of genus 1 with a rational point O.

Riemann-Roch gives functions $x, y \in k(E)$ regular except for double and triple poles at O. They generate $k(E)$ and satisfy (extended) Weierstrass equation

$$y^2 + a_1 xy + a_3 y = x^3 + a_2 x^2 + a_4 x + a_6 = 0$$

[sic: a_i, x, y of weight $i, 2, 3$] for some $a_i \in k$. Conversely, given a_i with $\Delta = \Delta(a_1, a_2, a_3, a_4, a_6)$ we get an elliptic curve.

Different choices of x, y give various a_i but same j-*invariant* $j = c_4^3/\Delta$, where $c_4 = (a_1^2 + 4a_2)^2 - 24(a_1 a_3 + 2a_4)$. Conversely if $j(E) = j(E')$ then $E \cong E'$ <u>over $\bar{k}$</u>. ["The j-line is a coarse moduli space for elliptic curves."]

If $6 \neq 0$ in k we can assume $a_1 = a_2 = a_3 = 0$, and then $j = 4 \cdot 12^3 a_4^3/(4a_4^3 + 27a_6^2)$. [For future use: $a_4 = 0 \Leftrightarrow j = 0$, and $a_6 = 0 \Leftrightarrow j = 1728$.]

An elliptic curve has a commutative **group law**: an algebraic map $E \times E \to E$, $(P,Q) \mapsto P+Q$ satisfying the axioms of an abelian group with origin O. It is characterized by the property that $P+Q+R=O$ <u>iff</u> $(P)+(Q)+(R) \sim 3(O)$. If $k \subseteq \mathbf{C}$ then $E(\mathbf{C}) \cong \mathbf{C}/\Lambda$ for some lattice $\Lambda \subset C$, and then the group law is consistent with addition in $\mathbf{C}/\Lambda$.

We study mathematical structures via maps between them that respect the structure. Here this means *isogenies*. An isogeny between elliptic curves $E, E'/k$ is an algebraic map $\phi : E \to E'$ such that $\phi(P+Q) = \phi(P)+\phi(Q)$ holds identically for $P, Q \in E$. Remarkably this condition holds for any algebraic map s.t. $\phi(O_E) = O_{E'}$. (So this framework accommodates classical work of Fermat, Euler, . . . on descents etc.)

For example, if $E = \mathbf{C}/\Lambda$ and $E' = \mathbf{C}/\Lambda'$ then ϕ must be of the form $z \mapsto c_\phi z$ for some c_ϕ such that $c_\phi \Lambda \subseteq \Lambda'$.

An elliptic curve has a commutative **group law**: an algebraic map $E \times E \to E$, $(P, Q) \mapsto P + Q$ satisfying the axioms of an abelian group with origin O. It is characterized by the property that $P + Q + R = O$ iff $(P) + (Q) + (R) \sim 3(O)$. If $k \subseteq \mathbf{C}$ then $E(\mathbf{C}) \cong \mathbf{C}/\Lambda$ for some lattice $\Lambda \subset C$, and then the group law is consistent with addition in $\mathbf{C}/\Lambda$.

We study mathematical structures via maps between them that respect the structure. Here this means *isogenies*. An isogeny between elliptic curves $E, E'/k$ is an algebraic map $\phi : E \to E'$ such that $\phi(P+Q) = \phi(P)+\phi(Q)$ holds identically for $P, Q \in E$. Remarkably this condition holds for any algebraic map s.t. $\phi(O_E) = O_{E'}$. (So this framework accommodates classical work of Fermat, Euler, ... on descents etc.)

For example, if $E = \mathbf{C}/\Lambda$ and $E' = \mathbf{C}/\Lambda'$ then ϕ must be of the form $z \mapsto c_\phi z$ for some c_ϕ such that $c_\phi \Lambda \subseteq \Lambda'$.

Given E and E', the isogenies $\phi : E \to E'$ themselves form an abelian group, denoted $\mathrm{Hom}(E, E')$. We allow ϕ to be defined over any algebraic extension of k. This group comes with a *degree* map $\deg : \mathrm{Hom}(E, E') \to \mathbf{Z}$ which is a positive-definite quadratic form. In the complex case, if $E = \mathbf{C}/\Lambda$ and $E' = \mathbf{C}/\Lambda'$ then $\deg(\phi) = [\Lambda' : c_\phi \Lambda]$ for nonzero ϕ. [This quadratic form is also an example of the canonical height on an elliptic surface, but that's for another VaNTAGe series.]

In the special case $E' = E$ we obtain the group $\mathrm{Hom}(E, E)$ of isogenies from E to itself, which has additional structure because such isogenies are closed also under composition. This gives $\mathrm{Hom}(E, E)$ the structure of a ring, called the *endomorphism ring* $\mathrm{End}(E)$; the product of $\phi_1, \phi_2 \in \mathrm{End}(E)$ is the composition $\phi_1 \circ \phi_2$. The identity map $1_E : E \to E$ is the unit of $\mathrm{End}(E)$. The remainder of these Preliminaries describes the classification of elliptic curves E/k by their endomorphism rings $\mathrm{End}(E)$.

Given E and E', the isogenies $\phi : E \to E'$ themselves form an abelian group, denoted $\text{Hom}(E, E')$. We allow ϕ to be defined over any algebraic extension of k. This group comes with a *degree* map $\deg : \text{Hom}(E, E') \to \mathbf{Z}$ which is a positive-definite quadratic form. In the complex case, if $E = \mathbf{C}/\Lambda$ and $E' = \mathbf{C}/\Lambda'$ then $\deg(\phi) = [\Lambda' : c_\phi \Lambda]$ for nonzero ϕ. [This quadratic form is also an example of the canonical height on an elliptic surface, but that's for another VaNTAGe series.]

In the special case $E' = E$ we obtain the group $\text{Hom}(E, E)$ of isogenies from E to itself, which has additional structure because such isogenies are closed also under composition. This gives $\text{Hom}(E, E)$ the structure of a ring, called the *endomorphism ring* $\text{End}(E)$; the product of $\phi_1, \phi_2 \in \text{End}(E)$ is the composition $\phi_1 \circ \phi_2$. The identity map $1_E : E \to E$ is the unit of $\text{End}(E)$. The remainder of these Preliminaries describes the classification of elliptic curves E/k by their endomorphism rings $\text{End}(E)$.

The map End$(E) \to \bar{k}$. An isogeny $\phi : E \to E'$ defined over some field $k_1 \supseteq k$ induces a map between the one-dim. Lie algebras of E, E', and pulls back to a map between the one-dim. spaces of holo. diffs. on E' and E. For $E' = E$ either of these constructions associates to ϕ the same element of k_1, and gives a canonical ring homomorphism ρ : End$_{k_1}(E) \to k_1$. Then ker ρ is the two-sided ideal of inseparable isogenies.

In char. zero ker $\rho = \{0\}$, whence End$_{k_1} \hookrightarrow k_1$, and in particular End$(E)$ is a commutative ring. Putting k (or at least $\mathbf{Q}(a_1, a_2, a_3, a_4, a_6)$) in $\mathbf{C}$, we get End$(E) \hookrightarrow \mathbf{C}$ with

$$\rho(\phi) = c_\phi, \qquad \deg \phi = [\Lambda : c_\phi \Lambda] = |\phi_c|^2$$

for all $\phi \in$ End(E). Since $\deg \phi \in \mathbf{Z}$ we conclude that either End$(E) = \mathbf{Z}$ or End(E) is a quadratic imaginary ring $O_{-D} = \mathbf{Z}[\frac{1}{2}(D + \sqrt{-D})]$. The former case is *ordinary*; the latter, *CM (complex multiplication)*. The beautiful theory of CM curves (and higher ab.vars.), and their moduli, is the main theme of this VaNTAGe series; we'll need only a small taste of it here.

The map $\mathrm{End}(E) \to \bar{k}$. An isogeny $\phi : E \to E'$ defined over some field $k_1 \supseteq k$ induces a map between the one-dim. Lie algebras of E, E', and pulls back to a map between the one-dim. spaces of holo. diffs. on E' and E. For $E' = E$ either of these constructions associates to ϕ the same element of k_1, and gives a canonical ring homomorphism $\rho : \mathrm{End}_{k_1}(E) \to k_1$. Then $\ker \rho$ is the two-sided ideal of inseparable isogenies.

In char. zero $\ker \rho = \{0\}$, whence $\mathrm{End}_{k_1} \hookrightarrow k_1$, and in particular $\mathrm{End}(E)$ is a commutative ring. Putting k (or at least $\mathbf{Q}(a_1, a_2, a_3, a_4, a_6)$) in $\mathbf{C}$, we get $\mathrm{End}(E) \hookrightarrow \mathbf{C}$ with

$$\rho(\phi) = c_\phi, \qquad \deg \phi = [\Lambda : c_\phi \Lambda] = |\phi_c|^2$$

for all $\phi \in \mathrm{End}(E)$. Since $\deg \phi \in \mathbf{Z}$ we conclude that either $\mathrm{End}(E) = \mathbf{Z}$ or $\mathrm{End}(E)$ is a quadratic imaginary ring $O_{-D} = \mathbf{Z}[\frac{1}{2}(D + \sqrt{-D})]$. The former case is *ordinary*; the latter, *CM (complex multiplication)*. The beautiful theory of CM curves (and higher ab.vars.), and their moduli, is the main theme of this VaNTAGe series; we'll need only a small taste of it here.

In char. $p > 0$ there can be inseparable isogenies $\phi \neq 0$ and noncommutative $\mathrm{End}(E)$. For example, assume $\mathrm{char}(k) \neq 2$, and let $E : y^2 = x^3 - x$ over a field that contains $i = \sqrt{-1}$. Then $\mathrm{End}(E)$ contains $\phi : (x, y) \mapsto (-x, iy)$ with $\rho(\phi) = i$ (because dx/y pulls back to $d(-x)/(iy) = i\,dx/y$). There's also the Frobenius isogeny $F : (x, y) \mapsto (x^p, y^p)$, with $\rho(F) = 0$. Then $Fi = (\frac{-1}{p}) iF$, so $\mathrm{End}(E)$ does not commute if $p \equiv 3 \bmod 4$.

Exercise: What happens for $y^2 = x^3 - 1$ and $(x, y) \mapsto (\zeta_3 x, y)$?

In general, in char. $p > 0$ the $\mathbf{Z}$-rank of $\mathrm{End}(E)$ can be 1, 2, or 4. The first case, equivalent to $\mathrm{End}(E) = \mathbf{Z}$, happens iff j is not in any finite field; that is, iff $j \notin \overline{\mathbf{F}_p}$. If $j \in \overline{\mathbf{F}_p}$ then usually $\mathrm{End}(E) \cong O_{-D}$ for some D, but there is a finite number of values of j, all in $\mathbf{F}_{p^2}$, for which $\mathrm{End}(E)$ has rank 4. The curve E is said to be *ordinary* in the former case, *supersingular* in the latter.

[NB such curves do not have geometric singularities . . .]

In char. $p > 0$ there can be inseparable isogenies $\phi \neq 0$ and noncommutative End(E). For example, assume char(k) $\neq 2$, and let $E : y^2 = x^3 - x$ over a field that contains $i = \sqrt{-1}$. Then End(E) contains $\phi : (x, y) \mapsto (-x, iy)$ with $\rho(\phi) = i$ (because dx/y pulls back to $d(-x)/(iy) = i\, dx/y$). There's also the Frobenius isogeny $F : (x, y) \mapsto (x^p, y^p)$, with $\rho(F) = 0$. Then $Fi = (\frac{-1}{p})iF$, so End(E) does not commute if $p \equiv 3 \bmod 4$.

Exercise: What happens for $y^2 = x^3 - 1$ and $(x, y) \mapsto (\zeta_3 x, y)$?

In general, in char. $p > 0$ the $\mathbf{Z}$-rank of End(E) can be 1, 2, or 4. The first case, equivalent to End(E) $= \mathbf{Z}$, happens iff j is not in any finite field; that is, iff $j \notin \overline{\mathbf{F}_p}$. If $j \in \overline{\mathbf{F}_p}$ then usually End(E) $\cong O_{-D}$ for some D, but there is a finite number of values of j, all in $\mathbf{F}_{p^2}$, for which End(E) has rank 4. The curve E is said to be *ordinary* in the former case, *supersingular* in the latter.

[NB such curves do not have geometric singularities . . .]

Why does $j \in \overline{\mathbf{F}_p}$ imply End$(E) \neq \mathbf{Z}$? If $j \in \overline{\mathbf{F}_p}$ then we can choose a_1, a_2, a_3, a_4, a_6 in some finite field $\mathbf{F}_q$, so again End(E) contains $F_q : (x, y) \mapsto (x^q, y^q)$. Usually that's enough because $F_q \notin \mathbf{Z}$. For instance, $\deg n = n^2$ for $n \in \mathbf{Z}$, while $\deg F_q = q$, so if $q = p^e$ with e odd then we're done. Curiously, if q is a square then $F_q = \pm q^{1/2}$ is possible — but then E is supersingular!

The general situation is described by Deuring (1941). Suppose $j \in \overline{\mathbf{F}_p}$. Then:

If E is ordinary, End(E) is an order in some imag.quad.field $\mathbf{Q}(\sqrt{-D})$ in which p splits, say $p = \mathfrak{p}\bar{\mathfrak{p}}$, with $\rho(\phi) = \phi \bmod \mathfrak{p}$ and $(F) = \mathfrak{p}^e$. In this case $(E, \text{End}(E))$ lifts to a CM curve over $\overline{\mathbf{Q}}$.

In supersingular case, . . .

Why does $j \in \overline{\mathbf{F}_p}$ imply End$(E) \neq \mathbf{Z}$? If $j \in \overline{\mathbf{F}_p}$ then we can choose a_1, a_2, a_3, a_4, a_6 in some finite field $\mathbf{F}_q$, so again End(E) contains $F_q : (x, y) \mapsto (x^q, y^q)$. Usually that's enough because $F_q \notin \mathbf{Z}$. For instance, $\deg n = n^2$ for $n \in \mathbf{Z}$, while $\deg F_q = q$, so if $q = p^e$ with e odd then we're done. Curiously, if q is a square then $F_q = \pm q^{1/2}$ is possible — but then E is supersingular!

The general situation is described by Deuring (1941). Suppose $j \in \overline{\mathbf{F}_p}$. Then:

If E is ordinary, End(E) is an order in some imag.quad.field $\mathbf{Q}(\sqrt{-D})$ in which p splits, say $p = \mathfrak{p}\bar{\mathfrak{p}}$, with $\rho(\phi) = \phi \bmod \mathfrak{p}$ and $(F) = \mathfrak{p}^e$. In this case $(E, \text{End}(E))$ lifts to a CM curve over $\overline{\mathbf{Q}}$.

In supersingular case, . . .

If E is supersingular then $\mathrm{End}(E)$ is a maximal order in the quaternion algebra $A_{p,\infty}$. Every $\phi \in \mathrm{End}(E)$ is either in $\mathbf{Z}$ or generates an order in some $\mathbf{Q}(\sqrt{-D})$ in which p is inert or ramified; if $\phi \notin \mathbf{Z}$ then (E, ϕ) again lifts to a CM curve over $\overline{\mathbf{Q}}$, but this time infinitely many different curves arise this way. Here ρ takes values in $\mathbf{F}_{p^2}$, and some power of F_q is in $\mathbf{Z}$.

Going the other way, if E is a CM curve over some number field K, with CM field $\mathrm{End}(E) \otimes_{\mathbf{Z}} \mathbf{Q} = \mathbf{Q}(\sqrt{-D})$, then $j = j_E$ is an algebraic integer. Thus for any prime $\mathfrak{p}$ of K above p we have a reduction $j \bmod \mathfrak{p}$. If $\bar{E}$ is an elliptic curve with that j-invariant over the fraction field, then $\bar{E}$ is ordinary if p splits in $\mathbf{Q}(\sqrt{-D})$, and supersingular if not.

Example ($-D = -4$): a curve in char. p with $j = 1728$ is supersingular iff $p \equiv 3 \bmod 4$ (or $p = 2$, as with $y^2 + y = x^3$).

If E is supersingular then End(E) is a maximal order in the quaternion algebra $A_{p,\infty}$. Every $\phi \in$ End(E) is either in $\mathbf{Z}$ or generates an order in some $\mathbf{Q}(\sqrt{-D})$ in which p is inert or ramified; if $\phi \notin \mathbf{Z}$ then (E, ϕ) again lifts to a CM curve over $\overline{\mathbf{Q}}$, but this time infinitely many different curves arise this way. Here ρ takes values in $\mathbf{F}_{p^2}$, and some power of F_q is in $\mathbf{Z}$.

Going the other way, if E is a CM curve over some number field K, with CM field End(E) $\otimes_{\mathbf{Z}} \mathbf{Q} = \mathbf{Q}(\sqrt{-D})$, then $j = j_E$ is an algebraic integer. Thus for any prime $\mathfrak{p}$ of K above p we have a reduction $j \bmod \mathfrak{p}$. If $\bar{E}$ is an elliptic curve with that j-invariant over the fraction field, then $\bar{E}$ is ordinary if p splits in $\mathbf{Q}(\sqrt{-D})$, and supersingular if not.

Example ($-D = -4$): a curve in char. p with $j = 1728$ is supersingular iff $p \equiv 3 \bmod 4$ (or $p = 2$, as with $y^2 + y = x^3$).

What if we start from two different CM invariants j_1, j_2, say 0 and -147197952000 (with $-D = -3$ and -67), and work in a field k of char. p where $j_1 = j_2$, i.e. modulo a factor p of $j_1 - j_2$? Then there's a curve E/k for which End(E) accommodates both O_{-D_1} and O_{-D_2}. So E must be supersingular, and moreover p can't be too large — turns out that p must divide $(D_1 D_2 - x^2)/4$ for some x, so in particular $p \leq D_1 D_2/4$.

Gross and Zagier (Crelle **355** (1984), 191–220) figured out the exact prime factorization of $\left|\text{Nm}(j - j')\right|$. For example, $147197952000 = 2^{15} 3^3 5^3 11^3 = 5280^3$. Amusing consequence: 1 mile $= e^{\pi\sqrt{67}/3}$ feet $+$ about 0.27 microns.

[Why $e^{\pi\sqrt{67}}$? The curve $\mathbf{C}/\Lambda$ is CM <u>iff</u> $\Lambda = \mathbf{Z}\omega_1 \oplus \mathbf{Z}\omega_2$ with $\tau := \omega_2/\omega_1$ imag.quadratic. Also $j = q^{-1} + 744 + O(q)$ with $q = e^{2\pi i\tau}$; now $\tau = (1 + \sqrt{-67})/2 \Longrightarrow q = -e^{-\pi\sqrt{67}}$, "etc."]

Further facts about supersingular curves:

• If $q = p^e$ then $E/\mathbf{F}_q$ is supersingular <u>iff</u> $|E(\mathbf{F}_q)| \equiv 1 \bmod p$. In particular if $e = 1$ (i.e. $q = p$) and $p \geq 5$ then $|E/\mathbf{F}_q| = q + 1$.

• The number of supersing. j-invariants in $\mathbf{F}_{p^2}$ is $p/12 + O(1)$; more precisely, $\lceil p/12 \rceil + \delta$ where $\delta = 0$ unless $p \equiv \pm 1 \bmod 12$ in which case $\delta = \mp 1$. Of those, $O(p^{1/2+\epsilon})$ are in $\mathbf{F}_p$; for $p > 2$ the number of supersingular $j \in \mathbf{F}_p$ is $\frac{1}{2}(H(-p) + H(-4p))$ [note $H(-p) = 0$ if $p \equiv 1 \bmod 4$]. Table:

p	2	3	5	7	11	13	17	19	23	29	31	37	41	43	47	$\cdots$
N_{p^2}	1	1	1	1	2	1	2	2	3	3	3	3	4	4	5	$\cdots$
N_p	1	1	1	1	2	1	2	2	3	3	3	1	4	2	5	$\cdots$

(You may recognize N_{p^2} also as $1 + g(\mathrm{X}_0(p))$, and N_p also as $\frac{1}{2}$ the number of fixed points of w_p. It may not look like $N_p = o(N_{p^2})$, but soon ... e.g. for $p = 971, 977, 983, 991, 997$ the counts are $30, 10, 27, 17, 7$ out of $82, 82, 83, 83, 83$.)

2. Primes of supersingular reduction

Now fix a curve E over $\mathbf{Q}$ (or more generally over some number field K). At all but finitely many primes p (or $\mathfrak{p}$), we can reduce E to get an elliptic curve $\bar{E}$ over the residue field with $j(\bar{E}) \equiv j(E) \bmod p$ (or $\bmod \mathfrak{p}$). Since $j(\bar{E})$ is in a finite field, $\bar{E}$ is at least CM. *How often is $\bar{E}$ supersingular?*

Some easy observations:

• Except for finitely many primes this depends only on the rational (or algebraic) number j_E.

• If E is already CM then we know $\bar{E}$ is supersingular iff the residue characteristic p is not split in the CM field. This happens for 1/2 of primes p by Čebotarev; the infinitude of such p is elementary, à la Euclid. For example, if $j = 1728$ (e.g. if E is $y^2 = x^3 - x$), we need $p \equiv -1 \bmod 4$, so factor $(4 \prod_{i=1}^{N} p_i) - 1$, etc.

But what if E is ordinary?

2. Primes of supersingular reduction

Now fix a curve E over $\mathbf{Q}$ (or more generally over some number field K). At all but finitely many primes p (or $\mathfrak{p}$), we can reduce E to get an elliptic curve $\bar{E}$ over the residue field with $j(\bar{E}) \equiv j(E) \bmod p$ (or $\bmod \mathfrak{p}$). Since $j(\bar{E})$ is in a finite field, $\bar{E}$ is at least CM. *How often is $\bar{E}$ supersingular?*

Some easy observations:

• Except for finitely many primes this depends only on the rational (or algebraic) number j_E.

• If E is already CM then we know $\bar{E}$ is supersingular iff the residue characteristic p is not split in the CM field. This happens for 1/2 of primes p by Čebotarev; the infinitude of such p is elementary, à la Euclid. For example, if $j = 1728$ (e.g. if E is $y^2 = x^3 - x$), we need $p \equiv -1 \bmod 4$, so factor $(4\prod_{i=1}^{N} p_i) - 1$, etc.

But what if E is ordinary?

What do we expect?

Over $\mathbf{Q}$, a "random" $\bar{E}$ mod p is supersingular with probability about $Cp^{-1/2}$ on average. So the number of such primes $p \leq x$, call it $\pi_0(x, E)$, should be asymptotic to

$$C \sum_{p \leq x} p^{-1/2} \sim C' \pi(x)/\sqrt{x} \sim C' x^{1/2}/\log x.$$

This is the Lang-Trotter conjecture, with C' replaced by some other $C_E > 0$ to account for the Galois structure of the torsion points of E. (E.g., if E has a rational 2-torsion point then $\#(\bar{E}(\mathbf{F}_p))$ is even, and thus likelier to equal $p+1$.)

This does seem roughly consistent with experiment; e.g. for $E = \mathrm{X}_1(11) : y^2 + y = x^3 - x^2$ the supersingular primes are

2, 19, 29, 199, 569, 809,
1289, 1439, 2539, 3319, 3559, 3919, 5519, 9419, 9539, 9929,

then 26 primes in $[10^4, 10^5]$, 57 primes in $[10^5, 10^6]$, "etc."

What do we expect?

Over $\mathbf{Q}$, a "random" $\bar{E}$ mod p is supersingular with probability about $Cp^{-1/2}$ on average. So the number of such primes $p \leq x$, call it $\pi_0(x, E)$, should be asymptotic to

$$C \sum_{p \leq x} p^{-1/2} \sim C' \pi(x)/\sqrt{x} \sim C' x^{1/2}/\log x.$$

This is the Lang-Trotter conjecture, with C' replaced by some other $C_E > 0$ to account for the Galois structure of the torsion points of E. (E.g., if E has a rational 2-torsion point then $\#(\bar{E}(\mathbf{F}_p))$ is even, and thus likelier to equal $p+1$.)

This does seem roughly consistent with experiment; e.g. for $E = \mathrm{X}_1(11) : y^2 + y = x^3 - x^2$ the supersingular primes are

2, 19, 29, 199, 569, 809,
1289, 1439, 2539, 3319, 3559, 3919, 5519, 9419, 9539, 9929,

then 26 primes in $[10^4, 10^5]$, 57 primes in $[10^5, 10^6]$, "etc."

What about E/K for a general number field K?

Depends on the exponent f in $\mathrm{Nm}(\mathfrak{p}) = p^f$. Write

$$\pi_0(x, E) = \sum_{f=1}^{[K:\mathbf{Q}]} \pi_0(x, E, f),$$

where $\pi_0(x, E, f)$ is the number of supersingular $\mathfrak{p}$ of norm $\leq x$ such that the residue field has degree f over the prime field. With finitely many exceptions, j_E generates the residue field, so $\pi_0(x, E, f) = O(1)$ for each $f > 2$. For $f = 1$ we expect $\sim C_{E,1} x^{1/2}/\log x$ as before — by Čebotarev a positive proportion of primes has $f = 1$. As for $f = 2$, a random $j \in \mathbf{F}_{p^2}$ is supersingular with probability about $1/(12p)$, so we expect $\pi_0(x, E, 2) \sim C_{E,2} \sum_{p \leq x} 1/p$ and $\sum_{p \leq x} 1/p \sim \log\log x$. So there should also be infinitely many supersingular primes of norm p^2, but *very* sparse.

What can we prove?

If E is not CM then certainly $\pi_0(x, E) = o(\pi(x))$, by applying Čebotarev to the torsion field $K(E[N!])$ and letting $N \to \infty$. The upper bound on $\pi_0(x, E)/\pi(x)$ decays very slowly, though Serre used sieve methods to show prove $\pi_0(x, E) = O(x^{3/4})$ conditional on GRH for $K(E[N!])$.

This is not special to "trace zero": for each fixed $t \in \mathbf{Z}$ we can get a similar upper bound on $\#\{p \leq x : |E/\mathbf{F}_p| = p+1-t\}$ (and likewise for general K).

The $t = 0$ case is special for lower bounds, though. We noted already that t must be even if E has a 2-torsion point; moreover if E is the CM curve $y^2 = x^3 - x$ then $t = \pm 2$ gives $p = n^2 + 1$ and that's a famous open problem.

Until 1986, the $t = 0$ question was open too...

Theorem. [NDE 1986, 1987] *Every $E/\mathbf{Q}$ has infinitely many supersingular primes. More generally, if E is defined over a number field and j_E has a real conjugate then E has infinitely many supersingular primes.*

Idea: Force $E \bmod p$ to be supersingular by making j_E congruent mod p to a CM j-invariant j_{-D} (so p is a factor of the numerator of $\mathrm{Nm}(j_E - j_{-D})$) with p not split in $\mathbf{Q}(\sqrt{-D})$.

Example: Let $E = \mathrm{X}_1(11)$ again. Then $j_E = -2^{12}/11$. Try $D = -67$. Calculate

$$j_E - j_{-67} = -\frac{2^{12}}{11} + 5280^3 = \frac{1619177467904}{11} = \frac{2^{12}395306999}{11},$$

and the prime 395306999 is inert in $\mathbf{Q}(\sqrt{-67})$ so it is a supersingular prime for E.

Problem: How to ensure at least one <u>new</u> supersingular prime factor of $\mathrm{Nm}(j_E - j_{-D})$?

As in Euclid's proof, we have a finite list $p_1, \ldots, p_n$ of primes to avoid, here the primes of bad reduction and the supersingular primes we already know. We avoid them by choosing D so that each p_i <u>does</u> split in $\mathbf{Q}(\sqrt{-D})$.

As in the Euclid variation for $p \equiv -1 \bmod 4$, we ensure that at least one prime factor of $\mathrm{Nm}(j_E - j_{-D})$ does not split in $\mathbf{Q}(\sqrt{-D})$ by arranging that the numerator of $\mathrm{Nm}(j_E - j_{-D})$ does not have $\chi_{-D} = +1$.

Fortunately, for each odd prime factor l of D the minimal polynomial P_{-D} of j_{-D} is either a square or $X - 1728$ times a square mod l. The unpaired factor $X - 1728$ arises <u>iff</u> $D = l$ or $D = 4l$. [This is shown using arguments similar to the upper bound on factors of $\mathrm{Nm}(j_{-D} - j_{-D'})$.] Example: $P_{-23}(X) \equiv (X - 1728)(X + 4)^2 \bmod 23$.

As in Euclid's proof, we have a finite list $p_1, \ldots, p_n$ of primes to avoid, here the primes of bad reduction and the supersingular primes we already know. We avoid them by choosing D so that each p_i <u>does</u> split in $\mathbf{Q}(\sqrt{-D})$.

As in the Euclid variation for $p \equiv -1 \bmod 4$, we ensure that at least one prime factor of $\mathrm{Nm}(j_E - j_{-D})$ does not split in $\mathbf{Q}(\sqrt{-D})$ by arranging that the numerator of $\mathrm{Nm}(j_E - j_{-D})$ does not have $\chi_{-D} = +1$.

Fortunately, for each odd prime factor l of D the minimal polynomial P_{-D} of j_{-D} is either a square or $X - 1728$ times a square mod l. The unpaired factor $X - 1728$ arises <u>iff</u> $D = l$ or $D = 4l$. [This is shown using arguments similar to the upper bound on factors of $\mathrm{Nm}(j_{-D} - j_{-D'})$.] Example: $P_{-23}(X) \equiv (X - 1728)(X + 4)^2 \bmod 23$.

It remains to control the sign of $P_{-D}(j_E)$. For $j_E \in \mathbf{Q}$ we use $P_{-l}P_{-4l}$, which has one large positive root $j(\sqrt{-l}\,)$ and one large negative root $j(\frac{1}{2}(1+\sqrt{-l}))$. Dirichlet's theorem provide infinitely many $l \equiv -1 \bmod 4$ such that each $\chi_{-l}(p_i) = +1$. A sufficiently large one makes $P_{-l}(j_E)P_{-4l}(j_E) < 0$, and we're soon done.

Mazur asked: what about other number fields?

So I've done all $E/\mathbf{Q}$ but only one number field . . .

If $[\mathbf{Q}(j_E) : \mathbf{Q}]$ is odd, so j_E has an odd number of real conjugates, the same argument works. If the number is even but positive, we need one more trick: instead of $P_{-l}P_{-4l}$, use $P_{l_1}P_{l_2}$, which has one large root and one that depends on l_1/l_2. By Dirichlet we can choose l_1/l_2 within ϵ. We adjust the ratio so exactly one factor of $\mathrm{Nm}(j_E - j_{-D})$ is negative, and proceed as before.

It remains to control the sign of $P_{-D}(j_E)$. For $j_E \in \mathbf{Q}$ we use $P_{-l}P_{-4l}$, which has one large positive root $j(\sqrt{-l}\,)$ and one large negative root $j(\frac{1}{2}(1+\sqrt{-l}))$. Dirichlet's theorem provide infinitely many $l \equiv -1$ mod 4 such that each $\chi_{-l}(p_i) = +1$. A sufficiently large one makes $P_{-l}(j_E)P_{-4l}(j_E) < 0$, and we're soon done.

Mazur asked: what about other number fields?

So I've done all $E/\mathbf{Q}$ but only one number field . . .

If $[\mathbf{Q}(j_E) : \mathbf{Q}]$ is odd, so j_E has an odd number of real conjugates, the same argument works. If the number is even but positive, we need one more trick: instead of $P_{-l}P_{-4l}$, use $P_{l_1}P_{l_2}$, which has one large root and one that depends on l_1/l_2. By Dirichlet we can choose l_1/l_2 within ϵ. We adjust the ratio so exactly one factor of $\mathrm{Nm}(j_E - j_{-D})$ is negative, and proceed as before.

It remains to control the sign of $P_{-D}(j_E)$. For $j_E \in \mathbf{Q}$ we use $P_{-l}P_{-4l}$, which has one large positive root $j(\sqrt{-l}\,)$ and one large negative root $j(\frac{1}{2}(1+\sqrt{-l}))$. Dirichlet's theorem provide infinitely many $l \equiv -1$ mod 4 such that each $\chi_{-l}(p_i) = +1$. A sufficiently large one makes $P_{-l}(j_E)P_{-4l}(j_E) < 0$, and we're soon done.

Mazur asked: what about other number fields?

So I've done all $E/\mathbf{Q}$ but only one number field . . .

If $[\mathbf{Q}(j_E) : \mathbf{Q}]$ is odd, so j_E has an odd number of real conjugates, the same argument works. If the number is even but positive, we need one more trick: instead of $P_{-l}P_{-4l}$, use $P_{l_1}P_{l_2}$, which has one large root and one that depends on l_1/l_2. By Dirichlet we can choose l_1/l_2 within ϵ. We adjust the ratio so exactly one factor of $\mathrm{Nm}(j_E - j_{-D})$ is negative, and proceed as before.

It remains to control the sign of $P_{-D}(j_E)$. For $j_E \in \mathbf{Q}$ we use $P_{-l}P_{-4l}$, which has one large positive root $j(\sqrt{-l}\,)$ and one large negative root $j(\frac{1}{2}(1+\sqrt{-l}))$. Dirichlet's theorem provide infinitely many $l \equiv -1$ mod 4 such that each $\chi_{-l}(p_i) = +1$. A sufficiently large one makes $P_{-l}(j_E)P_{-4l}(j_E) < 0$, and we're soon done.

Mazur asked: what about other number fields?

So I've done all $E/\mathbf{Q}$ but only one number field . . .

If $[\mathbf{Q}(j_E) : \mathbf{Q}]$ is odd, so j_E has an odd number of real conjugates, the same argument works. If the number is even but positive, we need one more trick: instead of $P_{-l}P_{-4l}$, use $P_{l_1}P_{l_2}$, which has one large root and one that depends on l_1/l_2. By Dirichlet we can choose l_1/l_2 within ϵ. We adjust the ratio so exactly one factor of $\mathrm{Nm}(j_E - j_{-D})$ is negative, and proceed as before.

Distribution of supersingular primes

Also as with Euclid, the proof is constructive, and gives effective lower bounds on $N_0(x, E)$, but these bounds grow *very* slowly — much worse even than the $\log\log x$ from Euclid. Even under GRH (more precisely, ERH for quadratic characters) the best lower bounds we have are $N_0(x, E) \gg \log\log x$ for all x and $N_0(x_n, E) \gg \log_n$ for an infinite sequence of x_n.

Curiously, this approach also gives an *upper* bound: we get $N_0(x, E) \ll_E x^{3/4}$ unconditionally for all non-CM curves E.

. . . and if j_E has no real conjugates?

For many totally complex j_E we can still prove infinitely many supersingular primes using $P_{-l}(j_E)$: all that's needed is a suitable factor of the numeratorof $j_E - 1728$. But there are some E for which $N_0(x,E)$ should grow much more slowly, because we can prove $N_0(x,E,1) = O(1)$ so $N_0(x,E,2)$ is our only hope.

Say that $j \in \mathbf{Q}(i)$ and E has a torsion group of order 4; for example, $E : y^2 = x^3 + (2i-4)x^2 + 4x$, so $j_E = 2^{14}/(i-4)$, and $(x,y) = (2, 2i+2)$ is a 4-torsion point. If rational prime p is $\mathfrak{p}\bar{\mathfrak{p}}$ in $\mathbf{Q}(i)$ then $p+1 \equiv 2 \bmod 4$, so neither $E \bmod \mathfrak{p}$ nor $E \bmod \bar{\mathfrak{p}}$ can be supersingular. So any supersingular p must be $-1 \bmod 4$; computation shows no such $p < 10^6$. Likewise for $E/\mathbf{Q}(\sqrt{-3})$ with a 3-torsion point, "etc."

But there are still many cases where $C_E > 0$ but we have no proof of $N_0(x,E) \to \infty$.

. . . and if j_E has no real conjugates?

For many totally complex j_E we can still prove infinitely many supersingular primes using $P_{-l}(j_E)$: all that's needed is a suitable factor of the numeratorof $j_E - 1728$. But there are some E for which $N_0(x, E)$ should grow much more slowly, because we can prove $N_0(x, E, 1) = O(1)$ so $N_0(x, E, 2)$ is our only hope.

Say that $j \in \mathbf{Q}(i)$ and E has a torsion group of order 4; for example, $E : y^2 = x^3 + (2i - 4)x^2 + 4x$, so $j_E = 2^{14}/(i - 4)$, and $(x, y) = (2, 2i+2)$ is a 4-torsion point. If rational prime p is $\mathfrak{p}\bar{\mathfrak{p}}$ in $\mathbf{Q}(i)$ then $p + 1 \equiv 2 \bmod 4$, so neither $E \bmod \mathfrak{p}$ nor $E \bmod \bar{\mathfrak{p}}$ can be supersingular. So any supersingular p must be $-1 \bmod 4$; computation shows no such $p < 10^6$. Likewise for $E/\mathbf{Q}(\sqrt{-3})$ with a 3-torsion point, "etc."

But there are still many cases where $C_E > 0$ but we have no proof of $N_0(x, E) \to \infty$.

3. Further variations

To apply this technique in other contexts, we need:

A moduli space, such as the j-line X(1);

An infinite family of subvarieties of codimension one, generalizing $P_{-D} = 0$;

And some luck in being able to arrange for $\chi(\ldots) \neq +1$.

More 1-dim. examples: some complex points on $X_0(p)/w$ (David Jao, 2003); rational points on some Shimura curves (Marat Sadykov, 2004). New ingredient: Hecke's angular equidistribution theorem.

Also, examples of Drinfeld modules with no supersingular reductions (even for $f > 1$; Bjorn Poonen, 1997).

Higher dimensions? Maybe stay tuned for the rest of VaNTAGe X. . .

3. Further variations

To apply this technique in other contexts, we need:

A moduli space, such as the j-line X(1);

An infinite family of subvarieties of codimension one, generalizing $P_{-D} = 0$;

And some luck in being able to arrange for $\chi(\ldots) \neq +1$.

More 1-dim. examples: some complex points on $X_0(p)/w$ (David Jao, 2003); rational points on some Shimura curves (Marat Sadykov, 2004). New ingredient: Hecke's angular equidistribution theorem.

Also, examples of Drinfeld modules with no supersingular reductions (even for $f > 1$; Bjorn Poonen, 1997).

Higher dimensions? Maybe stay tuned for the rest of VaNTAGe X. . .

3. Further variations

To apply this technique in other contexts, we need:

A moduli space, such as the j-line X(1);

An infinite family of subvarieties of codimension one, generalizing $P_{-D} = 0$;

And some luck in being able to arrange for $\chi(\ldots) \neq +1$.

More 1-dim. examples: some complex points on $X_0(p)/w$ (David Jao, 2003); rational points on some Shimura curves (Marat Sadykov, 2004). New ingredient: Hecke's angular equidistribution theorem.

Also, examples of Drinfeld modules with no supersingular reductions (even for $f > 1$; Bjorn Poonen, 1997).

Higher dimensions? Maybe stay tuned for the rest of VaNTAGe X. . .

3. Further variations

To apply this technique in other contexts, we need:

A moduli space, such as the j-line X(1);

An infinite family of subvarieties of codimension one, generalizing $P_{-D} = 0$;

And some luck in being able to arrange for $\chi(\ldots) \neq +1$.

More 1-dim. examples: some complex points on $X_0(p)/w$ (David Jao, 2003); rational points on some Shimura curves (Marat Sadykov, 2004). New ingredient: Hecke's angular equidistribution theorem.

Also, examples of Drinfeld modules with no supersingular reductions (even for $f > 1$; Bjorn Poonen, 1997).

Higher dimensions? Maybe stay tuned for the rest of VaNTAGe X. . .

THE END