Fallibility and other real-life problems

Everett W. Howe

Center for Communications Research, La Jolla

Conference on Open Questions in Cryptography and Number Theory
UC Irvine, 17–21 September 2018

email: however@alumni.caltech.edu Twitter: @howe

My connections with Alice

My connections with Alice

- In graduate school

My connections with Alice

- In graduate school
- In Ann Arbor

My connections with Alice

- In graduate school
- In Ann Arbor
- Looking for jobs

My connections with Alice

- In graduate school
- In Ann Arbor
- Looking for jobs
- As a colleague

My connections with Alice

- In graduate school
- In Ann Arbor
- Looking for jobs
- As a colleague
- As someone interested in improving the culture of mathematics

My connections with Alice

- In graduate school
- In Ann Arbor
- Looking for jobs
- As a colleague
- As someone interested in improving the culture of mathematics

Lots of people turn 60, but Alice has done more than that. . .

[Explanatory note: Here is where I mentioned Alice's contributions to mathematics and her support of more junior people — including me, over the years — and wished her a happy birthday.]

Part 1: Euler

An unexpected quotation

Ralph Waldo Emerson, in *Nature* (1836)

The astronomer, the geometer, rely on their irrefragable analysis, and disdain the results of observation. The sublime remark of Euler on his law of arches, “This will be found contrary to all experience, yet is true;” had already transferred nature into the mind, and left matter like an outcast corpse.

An unexpected quotation

Ralph Waldo Emerson, in *Nature* (1836)

The astronomer, the geometer, rely on their irrefragable analysis, and disdain the results of observation. The sublime remark of Euler on his law of arches, "This will be found contrary to all experience, yet is true;" had already transferred nature into the mind, and left matter like an outcast corpse.

[Here I mentioned that our colleagues in the humanities would say "there's a lot to unpack here."]

An unexpected quotation

Ralph Waldo Emerson, in *Nature* (1836)

The astronomer, the geometer, rely on their irrefragable analysis, and disdain the results of observation. The sublime remark of Euler on his law of arches, "This will be found contrary to all experience, yet is true;" had already transferred nature into the mind, and left matter like an outcast corpse.

[Here I mentioned that our colleagues in the humanities would say "there's a lot to unpack here."]

Many questions

- *Irrefragable*?

An unexpected quotation

Ralph Waldo Emerson, in *Nature* (1836)

The astronomer, the geometer, rely on their irrefragable analysis, and disdain the results of observation. The sublime remark of Euler on his law of arches, "This will be found contrary to all experience, yet is true;" had already transferred nature into the mind, and left matter like an outcast corpse.

[Here I mentioned that our colleagues in the humanities would say "there's a lot to unpack here."]

Many questions

- *Irrefragable*? (It means "irrefutable.")

An unexpected quotation

Ralph Waldo Emerson, in *Nature* (1836)

The astronomer, the geometer, rely on their irrefragable analysis, and disdain the results of observation. The sublime remark of Euler on his law of arches, "This will be found contrary to all experience, yet is true;" had already transferred nature into the mind, and left matter like an outcast corpse.

[Here I mentioned that our colleagues in the humanities would say "there's a lot to unpack here."]

Many questions

- *Irrefragable*? (It means "irrefutable.")
- *Emerson* was quoting *Euler*?!

An unexpected quotation

Ralph Waldo Emerson, in *Nature* (1836)

The astronomer, the geometer, rely on their irrefragable analysis, and disdain the results of observation. The sublime remark of Euler on his law of arches, "This will be found contrary to all experience, yet is true;" had already transferred nature into the mind, and left matter like an outcast corpse.

[Here I mentioned that our colleagues in the humanities would say "there's a lot to unpack here."]

Many questions

- *Irrefragable*? (It means "irrefutable.")
- *Emerson* was quoting *Euler*?!
- What is this "Law of arches"?

An unexpected quotation

Ralph Waldo Emerson, in *Nature* (1836)

The astronomer, the geometer, rely on their irrefragable analysis, and disdain the results of observation. The sublime remark of Euler on his law of arches, "This will be found contrary to all experience, yet is true;" had already transferred nature into the mind, and left matter like an outcast corpse.

[Here I mentioned that our colleagues in the humanities would say "there's a lot to unpack here."]

Many questions

- *Irrefragable*? (It means "irrefutable.")
- *Emerson* was quoting *Euler*?!
- What is this "Law of arches"?
- Did Euler really say this?

An unexpected quotation

Ralph Waldo Emerson, in *Nature* (1836)

The astronomer, the geometer, rely on their irrefragable analysis, and disdain the results of observation. The sublime remark of Euler on his law of arches, "This will be found contrary to all experience, yet is true;" had already transferred nature into the mind, and left matter like an outcast corpse.

[Here I mentioned that our colleagues in the humanities would say "there's a lot to unpack here."]

Many questions

- *Irrefragable*? (It means "irrefutable.")
- *Emerson* was quoting *Euler*?!
- What is this "Law of arches"?
- Did Euler really say this?
- If so, why?

Almost certainly, Emerson was not quoting Euler directly.

Samuel Taylor Coleridge, in *Aids to Reflection* (1825)

The celebrated Euler having demonstrated certain properties of Arches, adds: "All experience is in contradiction to this; but this is no reason for doubting its truth." The words sound paradoxical; but mean no more than this [. . .]

Cribbing from the Romantics

Almost certainly, Emerson was not quoting Euler directly.

Samuel Taylor Coleridge, in *Aids to Reflection* (1825)

The celebrated Euler having demonstrated certain properties of Arches, adds: "All experience is in contradiction to this; but this is no reason for doubting its truth." The words sound paradoxical; but mean no more than this [. . .]

Answers and questions

- ~~*Emerson*~~ *Coleridge* was quoting Euler?!

Cribbing from the Romantics

Almost certainly, Emerson was not quoting Euler directly.

Samuel Taylor Coleridge, in *Aids to Reflection* (1825)

The celebrated Euler having demonstrated certain properties of Arches, adds: "All experience is in contradiction to this; but this is no reason for doubting its truth." The words sound paradoxical; but mean no more than this [. . .]

Answers and questions

- ~~*Emerson*~~ *Coleridge* was quoting Euler?!
- ~~What is this "Law of arches"?~~ "Certain properties"?

Cribbing from the Romantics

Almost certainly, Emerson was not quoting Euler directly.

Samuel Taylor Coleridge, in *Aids to Reflection* (1825)

The celebrated Euler having demonstrated certain properties of Arches, adds: "All experience is in contradiction to this; but this is no reason for doubting its truth." The words sound paradoxical; but mean no more than this [. . .]

Answers and questions

- ~~*Emerson*~~ *Coleridge* was quoting Euler?!
- ~~What is this "Law of arches"?~~ "Certain properties"?
- Did Euler really say this?
- If so, why?

Enlightenment!

I doubt Coleridge read Euler. But I bet he read Voltaire.

Voltaire, in *Diatribe du docteur Akakia* (1752)

He [Euler] *asks forgiveness, on his knees, from all logicians for having written, on the occasion of a result contradicting his calculations: "Indeed, this [calculation] appears to be less in agreement with the truth; [. . .] In any case, the calculation rather than our judgement is to be trusted."*

Voltaire and Euler

Voltaire wrote the satirical *Diatribe du docteur Akakia* because he and Euler were on opposite sides of a contretemps in the court of Frederick the Great.

See: Paul Nahin, *Dr. Euler's fabulous formula* (Princeton University Press, 2006).

Euler: *Mechanica* (1736), Chapter 3, paragraph 272

Indeed, this [calculation] appears to be less in agreement with the truth; [. . .] *In any case, the calculation rather than our judgement is to be trusted.*

Euler: *Mechanica* (1736), Chapter 3, paragraph 272

Indeed, this [calculation] appears to be less in agreement with the truth; [. . .] *In any case, the calculation rather than our judgement is to be trusted.*

What is the context?

- Studying linear motion modeled by $\frac{d^2x}{dt^2} = kx^n$.
- What happens when $x = 0$? (n may be negative.)
- What happens when $x < 0$? (n may not be an integer.)
- For $n \leq -1$, Euler says the object will attain infinite speed as $x \to 0^+$...
- ...and then immediately reverse course once $x = 0$.

See: Eberhard Knobloch, "Euler and infinite speed", *Doc. Math.* 2012 (extra vol.)

Mathematical morals

What to take away from this story?

- In this case, Euler's model was not great.
- He derived questionable conclusions from this model.
- He did not accept criticism.

Mathematical morals

What to take away from this story?

- In this case, Euler's model was not great.
- He derived questionable conclusions from this model.
- He did not accept criticism.

Coleridge and Emerson *loved* Euler's quote, because:

- They liked the idea of creating truth from pure thought. . .
- . . . without regard to observation;
- . . . without having to *convince other people*.

Mathematical morals

What to take away from this story?

- In this case, Euler's model was not great.
- He derived questionable conclusions from this model.
- He did not accept criticism.

Coleridge and Emerson *loved* Euler's quote, because:

- They liked the idea of creating truth from pure thought...
- ...without regard to observation;
- ...without having to *convince other people*.

My takeaway

A proof is not a proof until you've convinced someone else.
Listen carefully to criticism.

Mathematical morals

What to take away from this story?

- In this case, Euler's model was not great.
- He derived questionable conclusions from this model.
- He did not accept criticism.

Coleridge and Emerson *loved* Euler's quote, because:

- They liked the idea of creating truth from pure thought. . .
- . . . without regard to observation;
- . . . without having to *convince other people*.

My takeaway

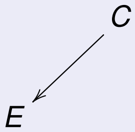
A proof is not a proof until you've convinced someone else.
Listen carefully to criticism.

[This point of view is certainly not new, or original to me. For an application to current events, see Cathy O'Neil's comments on the ABC conjecture.]

Part 2: Sleight of hand

Genus-2 double covers of elliptic curves

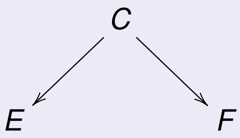
Given a genus-2 double cover of an elliptic curve $C \to E \ldots$



Genus-2 double covers of elliptic curves

Given a genus-2 double cover of an elliptic curve $C \to E$...

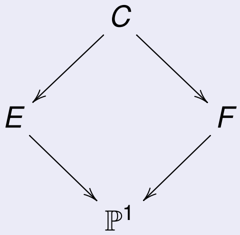
... there is a second double cover of an elliptic curve $C \to F$...



Background

Genus-2 double covers of elliptic curves

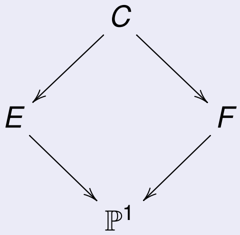
Given a genus-2 double cover of an elliptic curve $C \to E \ldots$
$\ldots$ there is a second double cover of an elliptic curve $C \to F \ldots$
$\ldots$ so that both fit into a V_4 Galois extension of $\mathbb{P}^1$.



Background

Genus-2 double covers of elliptic curves

Given a genus-2 double cover of an elliptic curve $C \to E$...
... there is a second double cover of an elliptic curve $C \to F$...
... so that both fit into a V_4 Galois extension of $\mathbb{P}^1$.



Old result: versions going back to Königsberger (J. Reine Angew. Math., 1867)

Communication

Some time ago. . .

A colleague at a university showed me a proof of something they were working on.

Something seemed “off” to me. No mistake jumped out, but. . .

I found a counterexample to a lemma.

Some time ago. . .

A colleague at a university showed me a proof of something they were working on.

Something seemed “off” to me. No mistake jumped out, but. . .

I found a counterexample to a lemma.

A conversation

Me: I think your lemma is wrong; here is a counterexample.

Communication

Some time ago. . .

A colleague at a university showed me a proof of something they were working on.

Something seemed "off" to me. No mistake jumped out, but. . .

I found a counterexample to a lemma.

A conversation

Me: I think your lemma is wrong; here is a counterexample.

Them: But I have a proof of the lemma.

Communication

Some time ago. . .

A colleague at a university showed me a proof of something they were working on.

Something seemed “off” to me. No mistake jumped out, but. . .

I found a counterexample to a lemma.

A conversation

Me: I think your lemma is wrong; here is a counterexample.

Them: But I have a proof of the lemma.

Me: Um, here’s a counterexample?

Communication

Some time ago…

A colleague at a university showed me a proof of something they were working on.

Something seemed "off" to me. No mistake jumped out, but…

I found a counterexample to a lemma.

A conversation

Me: I think your lemma is wrong; here is a counterexample.

Them: But I have a proof of the lemma.

Me: Um, here's a counterexample?

Them: But I have a proof.

Communication

Some time ago...

A colleague at a university showed me a proof of something they were working on.

Something seemed "off" to me. No mistake jumped out, but...

I found a counterexample to a lemma.

A conversation

Me: I think your lemma is wrong; here is a counterexample.

Them: But I have a proof of the lemma.

Me: Um, here's a counterexample?

Them: But I have a proof.

Me: $\langle \ldots \rangle$

A beautiful error

A construction

Them: I have an elliptic curve E...

$$E \to \mathbb{P}^1$$

A beautiful error

A construction

Them: I have an elliptic curve E. . .

. . . and I have constructed a genus-2 double cover $C \to E$.

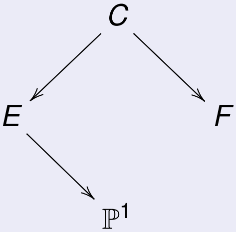
$$\begin{array}{ccc} & & C \\ & \swarrow & \\ E & & \\ & \searrow & \\ & & \mathbb{P}^1 \end{array}$$

A construction

Them: I have an elliptic curve E. . .

. . . and I have constructed a genus-2 double cover $C \to E$.

. . . therefore there is a second double cover $C \to F$.



A beautiful error

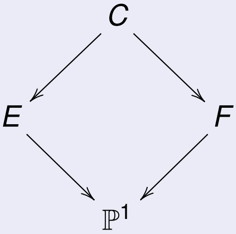
A construction

Them: I have an elliptic curve E...

... and I have constructed a genus-2 double cover $C \to E$.

... therefore there is a second double cover $C \to F$.

... that fits into a V_4 Galois extension of $\mathbb{P}^1$.



Mathematical morals

I made the error easier to see by drawing a diagram.

[Even so, not everyone in the audience spotted it. Hint: Which arrow gets drawn first?]

Mathematical morals

I made the error easier to see by drawing a diagram.

[Even so, not everyone in the audience spotted it. Hint: Which arrow gets drawn first?]

My colleague's argument was entirely in words.

Mathematical morals

I made the error easier to see by drawing a diagram.

[Even so, not everyone in the audience spotted it. Hint: Which arrow gets drawn first?]

My colleague's argument was entirely in words.

Not a single word of their argument was wrong.

Mathematical morals

I made the error easier to see by drawing a diagram.

[Even so, not everyone in the audience spotted it. Hint: Which arrow gets drawn first?]

My colleague's argument was entirely in words.

Not a single word of their argument was wrong.

This magic trick was created entirely unintentionally.

Mathematical morals

I made the error easier to see by drawing a diagram.

[Even so, not everyone in the audience spotted it. Hint: Which arrow gets drawn first?]

My colleague's argument was entirely in words.

Not a single word of their argument was wrong.

This magic trick was created entirely unintentionally.

My takeaway

- Errors can be subtle!
- It can be very hard to spot our own errors.
- We *need other people* to look at our proofs.

Part 3: An error in the wild

Background

Jeff Achter: What are some properties of principally-polarized abelian surfaces over finite fields that are rare, but not too rare?

If C is a genus-2 curve over $\mathbb{Q}$ we can study

$$\pi_T(C,x) = \#\left\{ p \le x : \begin{array}{l} \text{Jac } C \text{ has good reduction mod } p \\ \text{and the reduction has property } T \end{array} \right\}.$$

Let $P_T(q)$ be the probability that a randomly-chosen principally-polarized abelian surface over $\mathbb{F}_q$ has property T.

Naïvely expect $\pi_T(C,x) \sim \sum_{p<x} P_T(p)$.

Jeff Achter: What are some properties of principally-polarized abelian surfaces over finite fields that are rare, but not too rare?

If C is a genus-2 curve over $\mathbb{Q}$ we can study

$$\pi_T(C,x) = \#\left\{p \le x : \begin{array}{l}\text{Jac } C \text{ has good reduction mod } p\\ \text{and the reduction has property } T\end{array}\right\}.$$

Let $P_T(q)$ be the probability that a randomly-chosen principally-polarized abelian surface over $\mathbb{F}_q$ has property T.

Naïvely expect $\pi_T(C,x) \sim \sum_{p<x} P_T(p)$.

If $P_T(q) > c/q$, we expect $\pi_T(C,x)$ to grow visibly over ranges of x where we can actually compute it.

Instructive non-example

Consider the property T of *not being a Jacobian*.

Can show that $P_{\mathrm{nonJac}}(q) \approx 1/q$.

Naïvely, expect $\pi_{\mathrm{nonJac}}(C, x) \sim \sum_{p<x} 1/p \sim \log\log x$.

Instructive non-example

Consider the property T of *not being a Jacobian*.

Can show that $P_{\text{nonJac}}(q) \approx 1/q$.

Naïvely, expect $\pi_{\text{nonJac}}(C, x) \sim \sum_{p<x} 1/p \sim \log\log x$.

But $\operatorname{Jac} C$ is a Jacobian modulo p at every prime of good reduction for C, so $\pi_{\text{nonJac}}(C, x)$ is bounded for every curve C.

Instructive non-example

Consider the property T of *not being a Jacobian*.

Can show that $P_{\text{nonJac}}(q) \approx 1/q$.

Naïvely, expect $\pi_{\text{nonJac}}(C, x) \sim \sum_{p<x} 1/p \sim \log\log x$.

But $\operatorname{Jac} C$ is a Jacobian modulo p at every prime of good reduction for C, so $\pi_{\text{nonJac}}(C, x)$ is bounded for every curve C.

This example demonstrates:

- Why we would like properties T with $P_T(q) > c/q$, and
- That the naïve view is naïve.

Our choice

We looked at the property T of being *split over* $\mathbb{F}_q$.

Theorem (Achter-H. 2017)

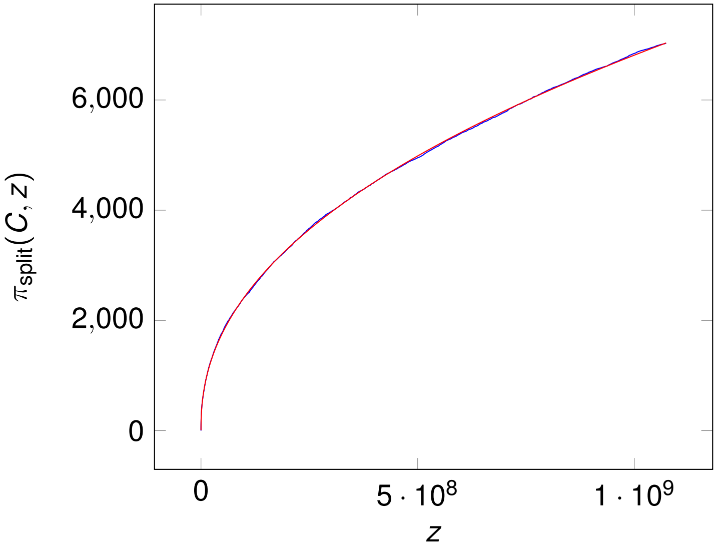
For all q we have

$$\frac{1}{(\log q)^3(\log\log q)^6} \ll P_{\text{split}}(q)\sqrt{q} \ll (\log q)^4(\log\log q)^2.$$

Conjecture (Achter-H. 2017)

Let J be the Jacobian of a genus-2 curve over $\mathbb{Q}$ with $\operatorname{End} J = \mathbb{Z}$. Then there is a constant $c_J > 0$ such that

$$\pi_{\text{split}}(J, x) \sim c_J \frac{\sqrt{x}}{\log x} \quad \textit{as } x \to \infty.$$



The blue curve is $\pi_{\text{split}}(C, z)$ for $C\colon\ y^2 = x^5 + x + 6$.

The red curve is $c\sqrt{z}/\log z$ with $c \approx 4.4651$.

[Here I thanked Drew Sutherland verbally — he provided programs and computer time to help produce this data.]

Open questions

1. What are interesting properties T of principally-polarized abelian surfaces with $P_T(q) > c/q$?
2. What are some approaches to proving the conjecture?
3. We look at surfaces that are split over $\mathbb{F}_q$. What about surfaces that are geometrically split?

Moduli spaces of supersingular genus-2 curves

The theorem above gives bounds for the number of non-simple principally-polarized abelian surfaces over $\mathbb{F}_q$.

A sub-problem

- Understand the moduli space of supersingular genus-2 curves.
- Moduli space of genus-2 curves: Subvariety of weighted projective space $[J_2 : J_4 : J_6 : J_8 : J_{10}]$.
- $J_{10} \neq 0$, plus single relation: $J_2 J_6 = J_4^2 + 4J_8$.

Moduli spaces of supersingular genus-2 curves

The theorem above gives bounds for the number of non-simple principally-polarized abelian surfaces over $\mathbb{F}_q$.

A sub-problem

- Understand the moduli space of supersingular genus-2 curves.
- Moduli space of genus-2 curves: Subvariety of weighted projective space $[J_2 : J_4 : J_6 : J_8 : J_{10}]$.
- $J_{10} \neq 0$, plus single relation: $J_2 J_6 = J_4^2 + 4J_8$.

The subvariety of supersingular curves is 1-dimensional, but the number of components grows with q.

Moduli spaces of supersingular genus-2 curves

The theorem above gives bounds for the number of non-simple principally-polarized abelian surfaces over $\mathbb{F}_q$.

A sub-problem

- Understand the moduli space of supersingular genus-2 curves.
- Moduli space of genus-2 curves: Subvariety of weighted projective space $[J_2 : J_4 : J_6 : J_8 : J_{10}]$.
- $J_{10} \neq 0$, plus single relation: $J_2 J_6 = J_4^2 + 4J_8$.

The subvariety of supersingular curves is 1-dimensional, but the number of components grows with q.

I wanted to look at case $q = 5$.

Computing equations for supersingular locus

Quick and dirty method

- Compute many supersingular genus-2 curves over $\mathbb{F}_{5^n}$.
- Compute their Igusa invariants $[J_2 : J_4 : J_6 : J_8 : J_{10}]$.
- Find low-degree polynomials vanishing at these points.
- Can prove guesses later.

Computing equations for supersingular locus

Quick and dirty method

- Compute many supersingular genus-2 curves over $\mathbb{F}_{5^n}$.
- Compute their Igusa invariants $[J_2 : J_4 : J_6 : J_8 : J_{10}]$.
- Find low-degree polynomials vanishing at these points.
- Can prove guesses later.

Manin and Yui

- Curve $C\colon y^2 = f = a_6x^6 + \cdots + a_0$ over $\mathbb{F}_{5^n}$.
- Let $g = f^2 = b_{12}x^{12} + \ldots + b_0$.
- Set $M = \begin{bmatrix} b_4 & b_3 \\ b_9 & b_8 \end{bmatrix}$ and $M^{(5)} = \begin{bmatrix} b_4^5 & b_3^5 \\ b_9^5 & b_8^5 \end{bmatrix}$.
- Yui, Manin: C is supersingular if and only if $MM^{(5)} = 0$.

Equations for the supersingular locus?

- Fit polynomials to many supersingular Igusa invariants in characteristic 5.
- In addition to $J_2 J_6 = J_4^2 + 4J_8$, found:
  - $J_4 = -J_2^2$.
  - Polynomial of weighted degree 1050 in J_2, J_6, and J_{10}.
- Highly singular subvariety of $\mathcal{M}_2$.
- Contradicts a result of Koblitz...

Equations for the supersingular locus?

- Fit polynomials to many supersingular Igusa invariants in characteristic 5.
- In addition to $J_2 J_6 = J_4^2 + 4J_8$, found:
  - $J_4 = -J_2^2$.
  - Polynomial of weighted degree 1050 in J_2, J_6, and J_{10}.
- Highly singular subvariety of $\mathcal{M}_2$.
- Contradicts a result of Koblitz...

Where was the problem?

- Had we misunderstood the result of Koblitz?
- Or is zero truly equal to one?

Equations for the supersingular locus?

- Fit polynomials to many supersingular Igusa invariants in characteristic 5.
- In addition to $J_2 J_6 = J_4^2 + 4J_8$, found:
  - $J_4 = -J_2^2$.
  - Polynomial of weighted degree 1050 in J_2, J_6, and J_{10}.
- Highly singular subvariety of $\mathcal{M}_2$.
- Contradicts a result of Koblitz...

Where was the problem?

- Had we misunderstood the result of Koblitz?
- Or is zero truly equal to one?
- We computed the zeta function of one of the curves that the Yui/Manin condition said was supersingular.

Equations for the supersingular locus?

- Fit polynomials to many supersingular Igusa invariants in characteristic 5.
- In addition to $J_2 J_6 = J_4^2 + 4J_8$, found:
  - $J_4 = -J_2^2$.
  - Polynomial of weighted degree 1050 in J_2, J_6, and J_{10}.
- Highly singular subvariety of $\mathcal{M}_2$.
- Contradicts a result of Koblitz. . .

Where was the problem?

- Had we misunderstood the result of Koblitz?
- Or is zero truly equal to one?
- We computed the zeta function of one of the curves that the Yui/Manin condition said was supersingular.
- It wasn't supersingular.

“Sign errors”

Manin (1961) and Yui (1978)

- Given a genus-g hyperelliptic curve $y^2 = f$ over $\mathbb{F}_{p^e}$, with Jacobian J.
- Let σ be the p-power Frobenius. There is a matrix M such that
  - the p-rank of J is the p-rank of $MM^{(\sigma)}M^{(\sigma^2)}\cdots M^{(\sigma^{g-1})}$.
  - the characteristic polynomial of p^e-Frobenius on J is related to the characteristic polynomial of $MM^{(\sigma)}M^{(\sigma^2)}\cdots M^{(\sigma^{e-1})}$.
- Yui gives a formula for M in terms of coefficients of $f^{(p-1)/2}$.

Yui’s formula for *M* does not work with these results. Need to:

- transpose M, or
- multiply the matrices in the opposite order, or
- replace σ with p-th root automorphism.

“Sign errors”

Manin (1961) and Yui (1978)

- Given a genus-g hyperelliptic curve $y^2 = f$ over $\mathbb{F}_{p^e}$, with Jacobian J.
- Let σ be the p-power Frobenius. There is a matrix M such that
  - the p-rank of J is the p-rank of $MM^{(\sigma)}M^{(\sigma^2)}\cdots M^{(\sigma^{g-1})}$.
  - the characteristic polynomial of p^e-Frobenius on J is related to the characteristic polynomial of $MM^{(\sigma)}M^{(\sigma^2)}\cdots M^{(\sigma^{e-1})}$.
- Yui gives a formula for M in terms of coefficients of $f^{(p-1)/2}$.

Yui’s formula for *M* does not work with these results. Need to:

- transpose M, or
- multiply the matrices in the opposite order, or
- replace σ with p-th root automorphism.

Note: For examples in Yui (1978), all M are *diagonal*, so mistake is not apparent.

Consequences

Equations for supersingular locus in $\mathcal{M}_2$ over $\mathbb{F}_{5^n}$

- Look at curves with $M^{(5)}M = 0$.
- In addition to $J_2J_6 = J_4^2 + 4J_8$, find:
  - $J_4 = -J_2^2$
  - $J_{10}J_2 = 3J_6^2 + 2J_6J_2^3 + 2J_2^6$
- Subvariety is image of $[2t^2 : t^4 : 3t + 4t^6 : 4t^3 + 3t^8 : 1]$.

Consequences

Equations for supersingular locus in $\mathcal{M}_2$ over $\mathbb{F}_{5^n}$

- Look at curves with $M^{(5)}M = 0$.
- In addition to $J_2J_6 = J_4^2 + 4J_8$, find:
  - $J_4 = -J_2^2$
  - $J_{10}J_2 = 3J_6^2 + 2J_6J_2^3 + 2J_2^6$
- Subvariety is image of $[2t^2 : t^4 : 3t + 4t^6 : 4t^3 + 3t^8 : 1]$.

Less pleasant consequences

- I *used* the incorrect criterion in an earlier paper!

Consequences

Equations for supersingular locus in $\mathcal{M}_2$ over $\mathbb{F}_{5^n}$

- Look at curves with $M^{(5)}M = 0$.
- In addition to $J_2J_6 = J_4^2 + 4J_8$, find:
  - $J_4 = -J_2^2$
  - $J_{10}J_2 = 3J_6^2 + 2J_6J_2^3 + 2J_2^6$
- Subvariety is image of $[2t^2 : t^4 : 3t + 4t^6 : 4t^3 + 3t^8 : 1]$.

Less pleasant consequences

- I *used* the incorrect criterion in an earlier paper!
- Panic.

Consequences

Equations for supersingular locus in $\mathcal{M}_2$ over $\mathbb{F}_{5^n}$

- Look at curves with $M^{(5)}M = 0$.
- In addition to $J_2J_6 = J_4^2 + 4J_8$, find:
  - $J_4 = -J_2^2$
  - $J_{10}J_2 = 3J_6^2 + 2J_6J_2^3 + 2J_2^6$
- Subvariety is image of $[2t^2 : t^4 : 3t + 4t^6 : 4t^3 + 3t^8 : 1]$.

Less pleasant consequences

- I *used* the incorrect criterion in an earlier paper!
- Panic.
- With the correct criterion, my proof still went through. Whew!

Ramifications

The results from *my* earlier paper still stood.

What about *other* papers that used the criterion?

Jeff and I decided to track down papers that cited Yui (1978) or Manin (1961).

Surely that wouldn't be *too* many papers. . .

A. Adolphson. The U_p-operator of Atkin on modular functions of level three. *Illinois J. Math.*, 24(1):49–60, 1980.

A. Álvarez. The p-rank of the reduction mod p of Jacobians and Jacobi sums. *Int. J. Number Theory*, 10(8):2097–2114, 2014.

M. Asada. On the action of the Frobenius automorphism on the pro-ℓ fundamental group. *Math. Z.*, 199(1):15–28, 1988.

M. H. Baker. Cartier points on curves. *Internat. Math. Res. Notices*, (7):353–370, 2000.

S. Ballet, C. Ritzenthaler, and R. Rolland. On the existence of dimension zero divisors in algebraic function fields defined over $\mathbb{F}_q$. *Acta Arith.*, 143(4):377–392, 2010.

E. Ballico. On the automorphisms of surfaces of general type in positive characteristic. II. *Atti Accad. Naz. Lincei Cl. Sci. Fis. Mat. Natur. Rend. Lincei (9) Mat. Appl.*, 5(1):63–68, 1994.

A. Bassa and P. Beelen. The Hasse-Witt invariant in some towers of function fields over finite fields. *Bull. Braz. Math. Soc. (N.S.)*, 41(4):567–582, 2010.

M. Bauer, M. J. Jacobson, Jr., Y. Lee, and R. Scheidler. Construction of hyperelliptic function fields of high three-rank. *Math. Comp.*, 77(261):503–530, 2008.

M. Bauer, E. Teske, and A. Weng. Point counting on Picard curves in large characteristic. *Math. Comp.*, 74(252):1983–2005, 2005.

J.-B. Bost. Algebraization, transcendence, and D–group schemes. *Notre Dame J. Form. Log.*, 54(3–4):377–434, 2013.

A. Bostan, P. Gaudry, and E. Schost. Linear recurrences with polynomial coefficients and computation of the Cartier–Manin operator on hyperelliptic curves. In *Finite fields and applications*, volume 2948 of Lecture Notes in Comput. Sci., pages 40–58. Springer, Berlin, 2004.

A. Bostan, P. Gaudry, and E. Schost. Linear recurrences with polynomial coefficients and application to integer factorization and Cartier–Manin operator. *SIAM J. Comput.*, 36(6):1777–1806, 2007.

I. I. Bouw, C. Diem, and J. Scholten. Ordinary elliptic curves of high rank over $\mathbb{F}_p(x)$ with constant j-invariant. *Manuscripta Math.*, 114(4):487–501, 2004.

B. Cais, J. S. Ellenberg, and D. Zureick–Brown. Random Dieudonné modules, random p-divisible groups, and random curves over finite fields. *J. Inst. Math. Jussieu*, 12(3):651–676, 2013.

G. Cardona and E. Nart. Zeta function and cryptographic exponent of supersingular curves of genus 2. In *Pairing-based cryptography — Pairing 2007*, volume 4575 of Lecture Notes in Comput. Sci., pages 132–151. Springer, Berlin, 2007.

J. W. S. Cassels. Diophantine equations with special reference to elliptic curves. *J. London Math. Soc.*, 41:193–291, 1966.

P. Cassou-Noguès, T. Chinburg, B. Erez, and M. J. Taylor. Derived category invariants and L-series. *J. Lond. Math. Soc. (2)*, 92(2):265–283, 2015.

W. Castryck, M. Streng, and D. Testa. Curves in characteristic 2 with non-trivial 2-torsion. *Adv. Math. Commun.*, 8(4):479–495, 2014.

J.-P. Cherdieu. Remarks on the zeta function of some diagonal hyperelliptic curves. *J. Pure Appl. Algebra*, 190(1–3):31–43, 2004.

G. Cornelissen, F. Oort, I. Bouw, T. Chinburg, C. Gasbarri, D. Glass, C. Lehr, M. Matignon, R. Pries, and S. Wewers. Problems from the Workshop on Automorphisms of Curves. *Rend. Sem. Mat. Univ. Padova*, 113:129–177, 2005.

B. Ditters and S. Hoving. Sur la composante connexe du module de Tate covariant de la famille des courbes, donnée par l'équation $y^2 = 1 + \mu x^N$. *C. R. Acad. Sci. Paris Sér. I Math.*, 306(14):621–624, 1988.

B. Ditters and S. J. Hoving. On the connected part of the covariant Tate p-divisible group and the ζ-function of the family of hyperelliptic curves $y^2 = 1 + \mu x^N$ modulo various primes. *Math. Z.*, 200(2):245–264, 1989.

E. J. Ditters. On the classification of commutative formal group laws over p-Hilbert domains and a finiteness theorem for higher Hasse–Witt matrices. *Math. Z.*, 202(1):83–109, 1989.

I. Dolgachev and D. Lehavi. On isogenous principally polarized abelian surfaces. In *Curves and abelian varieties*, volume 465 of Contemp. Math., pages 51–69. Amer. Math. Soc., Providence, RI, 2008.

A. Elkin. Hyperelliptic Jacobians with real multiplication. *J. Number Theory*, 117(1):53–86, 2006.

A. Elkin. The rank of the Cartier operator on cyclic covers of the projective line. *J. Algebra*, 327:1–12, 2011.

A. Elkin and R. Pries. Hyperelliptic curves with a-number 1 in small characteristic. *Albanian J. Math.*, 1(4):245–252, 2007.

A. Elkin and R. Pries. Ekedahl–Oort strata of hyperelliptic curves in characteristic 2. *Algebra Number Theory*, 7(3):507–532, 2013.

J. Estrada Sarlabous. On the Jacobian varieties of Picard curves defined over fields of characteristic $p > 0$. *Math. Nachr.*, 152:329–340, 1991.

S. Farnell and R. Pries. Families of Artin-Schreier curves with Cartier-Manin matrix of constant rank. *Linear Algebra Appl.*, 439(7):2158–2166, 2013.

F. Fité and A. V. Sutherland. Sato–Tate groups of $y^2 = x^8 + c$ and $y^2 = x^7 - cx$. In *Frobenius distributions: Lang–Trotter and Sato–Tate conjectures*, volume 663 of Contemp. Math., pages 103–126. Amer. Math. Soc., Providence, RI, 2016.

E. Furukawa, M. Kawazoe, and T. Takahashi. Counting points for hyperelliptic curves of type $y^2 = x^5 + ax$ over finite prime fields. In *Selected areas in cryptography*, volume 3006 of Lecture Notes in Comput. Sci., pages 26–41. Springer, Berlin, 2004.

S. D. Galbraith. *Mathematics of public key cryptography*. Cambridge University Press, Cambridge, 2012.

P. Gaudry and R. Harley. Counting points on hyperelliptic curves over finite fields. In *Algorithmic number theory (Leiden, 2000)*, volume 1838 of Lecture Notes in Comput. Sci., pages 313–332. Springer, Berlin, 2000.

A. Ghosh and K. Ward. The number of roots of polynomials of large degree in a prime field. *Int. Math. Res. Not. IMRN*, (4):898–926, 2015.

D. Glass and R. Pries. Hyperelliptic curves with prescribed p-torsion. *Manuscripta Math.*, 117(3):299–317, 2005.

H. Goodson. A complete hypergeometric point count formula for Dwork hypersurfaces. *J. Number Theory*, 179:142–171, 2017.

H. Goodson. Hypergeometric functions and relations to Dwork hypersurfaces. *Int. J. Number Theory*, 13(2):439–485, 2017.

R. Granger, F. Hess, R. Oyono, N. Thériault, and F. Vercauteren. Ate pairing on hyperelliptic curves. In *Advances in cryptology — EUROCRYPT 2007*, volume 4515 of Lecture Notes in Comput. Sci., pages 430–447. Springer, Berlin, 2007.

P. Guerzhoy. The Ramanujan differential operator, a certain CM elliptic curve and Kummer congruences. *Compos. Math.*, 141(3):583–590, 2005.

D. Harvey and A. V. Sutherland. Computing Hasse–Witt matrices of hyperelliptic curves in average polynomial time. *LMS J. Comput. Math.*, 17(suppl. A):257–273, 2014.

D. Harvey and A. V. Sutherland. Computing Hasse–Witt matrices of hyperelliptic curves in average polynomial time, II. In *Frobenius distributions: Lang–Trotter and Sato–Tate conjectures*, volume 663 of Contemp. Math., pages 127–147. Amer. Math. Soc., Providence, RI, 2016.

T. Hasegawa. Some remarks on superspecial and ordinary curves of low genus. *Math. Nachr.*, 286(1):17–33, 2013.

K.-i. Hashimoto and N. Murabayashi. Shimura curves as intersections of Humbert surfaces and defining equations of QM-curves of genus two. *Tohoku Math. J. (2)*, 47(2):271–296, 1995.

W. A. Hawkins, Jr. The étale cohomology of p-torsion sheaves. I. *Trans. Amer. Math. Soc.*, 301(1):163–188, 1987.

E. W. Howe. Supersingular genus-2 curves over fields of characteristic 3. In *Computational arithmetic geometry*, volume 463 of Contemp. Math., pages 49–69. Amer. Math. Soc., Providence, RI, 2008.

T. Ibukiyama, T. Katsura, and F. Oort. Supersingular curves of genus two and class numbers. *Compositio Math.*, 57(2):127–152, 1986.

F. A. Izadi and V. K. Murty. Counting points on an abelian variety over a finite field. In *Progress in cryptology — INDOCRYPT 2003*, volume 2904 of Lecture Notes in Comput. Sci., pages 323–333. Springer, Berlin, 2003.

N. M. Katz. Algebraic solutions of differential equations (p-curvature and the Hodge filtration). *Invent. Math.*, 18:1–118, 1972.

H. A. W. M. Kneppers. The Hasse–Witt matrix of a formal group. *Math. Z.*, 189(2):151–165, 1985.

T. Kodama and T. Washio. On class numbers of hyperelliptic function fields with Hasse–Witt-invariant zero. *Arch. Math. (Basel)*, 49(3):208–213, 1987.

T. Kodama and T. Washio. Hasse–Witt matrices of Fermat curves. *Manuscripta Math.*, 60(2):185–195, 1988.

T. Kodama and T. Washio. A family of hyperelliptic function fields with Hasse–Witt-invariant zero. *J. Number Theory*, 36(2):187–200, 1990.

M. Kudo and S. Harashita. Superspecial curves of genus 4 in small characteristic. *Finite Fields Appl.*, 45:131–169, 2017.

C. Lennon. Trace formulas for Hecke operators, Gaussian hypergeometric functions, and the modularity of a threefold. *J. Number Theory*, 131(12):2320–2351, 2011.

D. J. Madden. Arithmetic in generalized Artin–Schreier extensions of $k(x)$. *J. Number Theory*, 10(3):303–323, 1978.

K. Matsuo, J. Chao, and S. Tsujii. An improved baby step giant step algorithm for point counting of hyperelliptic curves over finite fields. In *Algorithmic number theory (Sydney, 2002)*, volume 2369 of Lecture Notes in Comput. Sci., pages 461–474. Springer, Berlin, 2002.

K. Matsuo, J. Chao, and S. Tsujii. Baby step giant step algorithms in point counting of hyperelliptic curves. *IEICE Trans. Fundamentals*, E86-A(5):1127–1134, 2003.

B. Mazur. Frobenius and the Hodge filtration. *Bull. Amer. Math. Soc.*, 78:653–667, 1972.

L. Miller. Curves with invertible Hasse-Witt-matrix. *Math. Ann.*, 197:123–127, 1972.

L. Miller. Über gewöhnliche Hyperflächen. I. *J. Reine Angew. Math.*, 282:96–113, 1976.

L. Miller. Über gewöhnliche Hyperflächen. II. *J. Reine Angew. Math.*, 283/284:402–420, 1976.

N. O. Nygaard. Slopes of powers of Frobenius on crystalline cohomology. *Ann. Sci. École Norm. Sup. (4)*, 14(4):369–401 (1982), 1981.

N. O. Nygaard. On supersingular abelian varieties. In *Algebraic geometry (Ann Arbor, Mich., 1981)*, volume 1008 of Lecture Notes in Math., pages 83–101. Springer, Berlin, 1983.

L. D. Olson. Hasse invariants and anomalous primes for elliptic curves with complex multiplication. *J. Number Theory*, 8(4):397–414, 1976.

Ë. Onishi. Generalized Bernoulli–Hurwitz numbers and universal Bernoulli numbers. *Uspekhi Mat. Nauk*, 66(5):47–108, 2011.

Ë. Onishi. Generalized Bernoulli–Hurwitz numbers and universal Bernoulli numbers. *Russian Math. Surveys*, 66(5):871–932, 2011.

A. I. Pacheco. A note on relations between the zeta-functions of Galois coverings of curves over finite fields. *Canad. Math. Bull.*, 33(3):282–285, 1990.

R. J. Pries. Jacobians of quotients of Artin-Schreier curves. In *Recent progress in arithmetic and algebraic geometry*, volume 386 of Contemp. Math., pages 145–156. Amer. Math. Soc., Providence, RI, 2005.

R. Pries. The p-torsion of curves with large p-rank. *Int. J. Number Theory*, 5(6):1103–1116, 2009.

R. Pries and K. Stevenson. A survey of Galois theory of curves in characteristic p. In *WIN — Women in numbers*, volume 60 of Fields Inst. Commun., pages 169–191. Amer. Math. Soc., Providence, RI, 2011.

H.-G. Rück. Class groups and L-series of function fields. *J. Number Theory*, 22(2):177–189, 1986.

P. Sarkar and S. Singh. A simple method for obtaining relations among factor basis elements for special hyperelliptic curves. *Appl. Algebra Engrg. Comm. Comput.*, 28(2):109–130, 2017.

J. H. Silverman. *The arithmetic of elliptic curves*, volume 106 of Grad. Texts in Math. Springer, Dordrecht, second edition, 2009.

G. Sohn. Computing the number of points on genus 3 hyperelliptic curves of type $Y^2 = X^7 + aX$ over finite prime fields. *J. Appl. Math. Inform.*, 32(1-2):17–26, 2014.

G. Sohn and H. Kim. Explicit bounds of polynomial coefficients and counting points on Picard curves over finite fields. *Math. Comput. Modelling*, 49(1-2):80–87, 2009.

K.-O. Stöhr and J. F. Voloch. A formula for the Cartier operator on plane algebraic curves. *J. Reine Angew. Math.*, 377:49–64, 1987.

F. J. Sullivan. p-torsion in the class group of curves with too many automorphisms. *Arch. Math. (Basel)*, 26:253–261, 1975.

Y. Sung. Rational points over finite fields on a family of higher genus curves and hypergeometric functions. *Taiwanese J. Math.*, 21(1):55–79, 2017.

S. Tafazolian. A family of maximal hyperelliptic curves. *J. Pure Appl. Algebra*, 216(7):1528–1532, 2012.

Y. Takeda. Groups of Russell type and Tango structures. In *Affine algebraic geometry*, volume 54 of CRM Proc. Lecture Notes, pages 327–334. Amer. Math. Soc., Providence, RI, 2011.

Y. Takeda and K. Yokogawa. Pre-Tango structures on curves. *Tohoku Math. J. (2)*, 54(2):227–237, 2002.

Y. Takizawa. Some remarks on the Picard curves over a finite field. *Math. Nachr.*, 280(7):802–811, 2007.

D. L. Ulmer. On universal elliptic curves over Igusa curves. *Invent. Math.*, 99(2):377–391, 1990.

R. C. Valentini. Hyperelliptic curves with zero Hasse–Witt matrix. *Manuscripta Math.*, 86(2):185–194, 1995.

T. Washio. On class numbers of algebraic function fields defined by $y^2 = x^5 + ax$ over GF(p). *Arch. Math. (Basel)*, 41(6):509–516, 1983.

N. Yui. On the Jacobian variety of the Fermat curve. *J. Algebra*, 65(1):1–35, 1980.

N. Yui. The arithmetic of the product of two algebraic curves over a finite field. *J. Algebra*, 98(1):102–142, 1986.

N. Yui. Jacobi quartics, Legendre polynomials and formal groups. In *Elliptic curves and modular forms in algebraic topology (Princeton, NJ, 1986)*, volume 1326 of Lecture Notes in Math., pages 182–215. Springer, Berlin, 1988.

L. Zapponi. On the 1-pointed curves arising as étale covers of the affine line in positive characteristic. *Math. Z.*, 258(4):711–727, 2008.

Y. G. Zarhin. Non-supersingular hyperelliptic Jacobians. *Bull. Soc. Math. France*, 132(4):617–634, 2004.

A total of 91 papers

Many papers were still OK

- Cited Manin and Yui as general references, no results quoted.
- Or, results *were* quoted, but:
  - The quoted results were not applied.
  - The quoted results did not contain errors.
  - Errors were silently corrected.
- Or, incorrect results *were* applied, but the formulas worked anyway:
  - The matrix M was diagonal.
  - M had entries in $\mathbb{F}_p$ or $\mathbb{F}_{p^2}$, so $M^\sigma = M^{\sigma^{-1}}$.
  - ...

But eight papers required a closer look.

Results

We contacted Manin, Yui, and the authors of the eight papers.

They were generous, polite, and glad to learn of the problem.

See the paper that Jeff and I wrote about this for more details.

My takeaway

- Mistakes can sit unnoticed for a long time.
- Mistakes can spread.

Part 4: Alice in the real world

Lessons from mistakes

- Everyone makes mistakes.
- They can be hard to see ourselves.
- They can remain there for years.
- Their effects can be widespread.
- To find them and fix them, we need to
    - listen to criticism;
    - think differently than we may be used to;
    - not get defensive.

Alice's adventures in numberland

For about a year now, Alice has been blogging about stories from her life.

To me, some of these stories seem to be about mistakes:
Mistakes by mathematicians, but not about mathematics.

Among the many experiences she writes of, some tell of mistakes — *injustices* is a better word — about how women are treated in our profession.

A gift

For some of us, Alice's blog is the gift of a different perspective.

In my life, I've seen some of these injustices firsthand, from the low-level everyday ones to the rare and extraordinary ones. [Some stories were mentioned here.]

But I haven't seen them all.

- Sometimes, I am not in the room to see.
- Sometimes, I am present, but do not notice.
- Sometimes, I make mistakes myself, despite my best intentions.

Alice's blog helps me be aware of problems I might otherwise miss —
and there are still *more* voices to listen to, because sexism is not the only problem.

A referee report

As mathematicians, we value:

- the colleagues who read and comment on our preprints;
- the referees who check our reasoning and catch mistakes;
- the editors who improve our writing.

We should also value the people who tell stories of how our community fails to live up to our highest values.

Open question, closing hope

An open question:

How do we want the community of mathematicians to be experienced — by all of its members?

A closing hope

May we hear and appreciate criticisms of our community...
May we acknowledge the injustices that occur in our profession...
And may we *actively do something to remedy them*.