The Weil Conjectures via Riemann - Roch.
(Source: Iwaniec + Kowalski, 11.10)
Given an EC $E/\mathbb{F}_q$. We want to prove that

$$Z(E;\mathbb{F}_q) = \frac{1 - aT + qT^2}{(1-T)(1-qT)} \qquad a := q+1-\#E(\mathbb{F}_q),$$

where

$$Z(E;\mathbb{F}_q) = \exp\left(\sum_{n\geq 1} \frac{|E(\mathbb{F}_{q^n})|}{n} T^n\right) = \prod_{x\in|E|} \left(1 - T^{\deg(x)}\right)^{-1}$$

product over closed points of E:
Galois orbits of $x_0 \in E(\overline{\mathbb{F}_q})$
$\deg(x)$ = cardinality of orbit.

Also have $Z(E;\mathbb{F}_q) = \sum_D T^{\deg(D)}$ sum over effective divisors
(nonnegative formal sums of closed points).

We will address the problem in this way, and further write

$$Z(E;\mathbb{F}_q) = 1 + \sum_{d\geq 1} T^d \sum_{\substack{D\geq 0 \\ \deg(D)=d}} 1$$

same as "effective" above.

<u>Claim</u>. $\displaystyle\sum_{\substack{D\geq 0\\ \deg(D)=d}} 1 = \#E(\mathbb{F}_q)\cdot \frac{q^d-1}{q-1}$.

(Note: when $d=1$, just says $\displaystyle\sum_{\substack{D\geq 0\\ \deg(D)=1}} 1 = \#E(\mathbb{F}_q)$, which is a tautology.

21.2

Given the claim,

$$Z(E;\mathbb{F}_q) = 1 + \sum_{d \geq 1} T^d \cdot \#E(\mathbb{F}_q) \cdot \frac{q^d - 1}{q-1}$$

$$= 1 + \frac{\#E(\mathbb{F}_q)}{q-1} \cdot \sum_{d \geq 1} T^d (q^d - 1)$$

$$= 1 + \frac{\#E(\mathbb{F}_q)}{q-1} \left(\sum_{d \geq 1} (Tq)^d - \sum_{d \geq 1} T^d \right)$$

$$= 1 + \frac{\#E(\mathbb{F}_q)}{q-1} \left(\frac{Tq}{1-Tq} - \frac{T}{1-T} \right)$$

$$\cancel{= 1 + \#E(\mathbb{F}_q) \cdot qT}$$

$$= 1 + \frac{\#E(\mathbb{F}_q)}{q-1} \cdot \frac{qT(1-T) - T(1-qT)}{(1-T)(1-qT)}$$

$$= 1 + \frac{\#E(\mathbb{F}_q)}{q-1} \cdot \frac{(q-1)T}{(1-T)(1-qT)}$$

$$= \frac{(1-(q+1)T + qT^2) + \#E(\mathbb{F}_q) \cdot T}{(1-T)(1-qT)}$$ QED.

So we want to prove the claim.

21.3.

Recall, for any divisor $D \in \mathrm{Div}(E)$, we define

$$L(D) := \{0\} \cup \{ f \in \underbrace{\bar{k}(E)} \mid (f) + D \geq 0 \}.$$

Recall: If E is embedded in $\mathbb{P}^2(k)$,

$$\bar{k}[E] = \frac{(\text{homo polys in } X, Y, Z)}{\text{those vanishing on } E}$$

$\bar{k}(E)$ = fraction field of this.

Functions on E whose poles are at worst at D.

This is a vector space.

$\mathbb{P}(L(D)) = L(D)/\text{scalars}$.

We have a bijection

$$\mathbb{P}(L(D)) \longrightarrow \{\text{effective divisors linearly equiv to } D\}$$

$$\varphi \longrightarrow (\varphi) + D.$$

Why surjective? Def. of linear equivalence means

$E \sim D$ if $E - D = \mathrm{div}(\varphi)$ for some $\varphi \in \bar{k}(E)$.

So this is tautological.

why injective? If $(\varphi) + D = (\psi) + D$ then $(\varphi) = (\psi)$

$\frac{\varphi}{\psi}$ is a rational fn. with no zeroes or poles.

22 starts here.

None exist other than the constants.

Why? Could RR this.

Direct argument: assume $E: y^2 = x^3 + ax + b$

(or $y^2 + c_1 xy + \cdots$ really not necessary)

In the affine patch $z = 1$, can write

$$\frac{\varphi}{\psi} = \frac{g_1(x) + y g_2(x)}{g_3(x) + y g_4(x)}.$$

Polynomials g_1, g_2, g_3, g_4. (Use equation of E to subst for y^2).

21.4. (= 22.1 essentially)

Now we have, in the denominator, $y = \dfrac{-g_3(x)}{g_4(x)}$

Substitute in the equation for the elliptic curve. It has solutions $x \in \overline{\mathbb{F}_q}$ by the "fundamental thm of algebra".

But the top and bottom have the same solutions. Forces them to be the same up to a scalar. So $\frac{y}{4} \in \overline{\mathbb{F}_q}^{\times}$.

By Riemann-Roch, if D has degree ≥ 1,

$$\ell(D) := \dim L(D) = \deg(D).$$

(This is particular to elliptic curves.)

Rationality. All of our AG assumed our field was algebraically closed. That doesn't help us.

Def. A point or divisor on E is called k-rational if it is fixed by $\mathrm{Gal}(\bar{k}/k)$.

For a point, this means coordinates are in k.
For a divisor, all conjugates of any point must be counted with multiplicity.

So, by definition, these correspond to sums of closed pts. on E/k.

Example. $V = V(x^2 + y^2 + 1) \subseteq \mathbb{A}^2(\mathbb{R})$.
$\{(i,0), (-i,0)\}$ is a closed point over $\mathbb{R}$, of deg 2, and $(i,0) + (-i,0)$ is the corresponding divisor on $V(\mathbb{C})$. $\mathrm{Gal}(\mathbb{C}/\mathbb{R}) = \{1, \text{cpx conj.}\}$ and c.c. fixes this divisor.

Now define (if D is k-rational, i.e. defined $/k$)

$$L_k(D) := \{0\} \cup \{ f \in k(E) \mid (f) + D \geq 0 \},$$

$$\ell_k(D) := \dim L_k(D).$$

Then $\ell_k(D) \leq \ell(D)$ $(= \ell_{\bar{k}}(D))$ because if various f are k-linearly independent then they are still so over $\bar{k}$.

Theorem. If D is k-rational then

$$\ell_k(D) = \ell(D).$$

See Sil. II. 5.8.1. Hilbert 90!

Indeed if V is a $\bar{k}$-vector space with an action of $\mathrm{Gal}(\bar{k}/k)$, there is a basis of G_k-invariant elements.

Equivalently, $\dim_k V^{G_k} = \dim_{\bar{k}} V$.

And so $$|L_k(D)| = q^{\ell_k(D)} \overset{\text{rationality}}{=} q^{\ell(D)} \overset{\text{Riemann-Roch}}{=} q^{\deg(D)}$$

and so $$|\mathbb{P}(L_k(D))| = \frac{q^{\deg(D)} - 1}{q - 1}$$

and so $\displaystyle\sum_{\substack{D \geq 0 \\ \deg(D) = d}} 1$ is this times the number of equivalence classes of $\mathbb{F}_q$-rational divisors of degree d.

21.6.

Proposition. Let $h_d(E)$ be the number of equiv classes of $\mathbb{F}_q$-rational divisors of degree d. Then $h_d(E) = h_0(E)$ $\forall d$, and $|h_d(E)| = |E(\mathbb{F}_q)|$.

Proof. The first claim is easy. Pick any divisor D_d of degree d, then

$$D \sim E \longmapsto D + D_d \sim E + D_d.$$

In degree 0, the classes $P - \infty$ are all inequivalent, had an isomorphism

$$E \longrightarrow \mathrm{Pic}^0(E)$$
$$P \longrightarrow (P) - (\infty).$$

Suppose you have $(P_1) + (P_2) - (P_3) - (P_4)$

can replace with $-(P_{1,2}) + (P_{3,4})$

where $P_1, P_2, P_{1,2}$ are the three collinear points on the line through P_1 and P_2.

22.1 = 23.1

Theorem. Let $E/\mathbb{F}_q$ be an EC. Then
$$\left| \# E(\mathbb{F}_q) - q - 1 \right| \le 2\sqrt{q}.$$

Idea of the proof. Want to do AG, so work in $\overline{\mathbb{F}_q}$.

~~A point~~ An element $x \in \overline{\mathbb{F}_q}$ is in fact in $\mathbb{F}_q$ if and only if $x^q = x$.

Indeed, for each $n \ge 1$,
$$\mathrm{Gal}(\mathbb{F}_{q^n}/\mathbb{F}_q) \cong \mathbb{Z}/n \text{ and is generated by}$$
the Frobenius endomorphism $x \longrightarrow x^q$.

By Galois theory its fixed field is $\mathbb{F}_q$.

If $E/\mathbb{F}_q$ is an EC, then we obtain the Frobenius map on E (an endomorphism)
$$\mathrm{Frob} : E \longrightarrow E$$
$$(x,y) \longrightarrow (x^q, y^q)$$
whose fixed points are precisely the $\mathbb{F}_q$-rational points.

So
$$\# E(\mathbb{F}_q) = \left| \mathrm{Ker}(1 - \mathrm{Frob}) \right|$$
where $1 - \mathrm{Frob}$ is also an endomorphism.

22.2 = 23.2

The idea: if $\phi : E \to E$ is any endomorphism, there exists a dual $\hat{\phi} : E \to E$ with $\phi \circ \hat{\phi} = \hat{\phi} \circ \phi = [\deg \phi]$.

(Essentially $\deg \phi = |\mathrm{Ker}\, \phi|$ but there are technicalities.)

This commutes with addition, i.e. $\widehat{\phi + \psi} = \hat{\phi} + \hat{\psi}$.
(This is not trivial)

So $\# E(\mathbb{F}_q) = \widehat{(1 - \mathrm{Frob})} \circ (1 - \mathrm{Frob})$ (i.e. this is the endomorphism mult. by $\# E(\mathbb{F}_q)$)

$= (1 - \widehat{\mathrm{Frob}}) \circ (1 - \mathrm{Frob})$

$= 1 - (\widehat{\mathrm{Frob}} + \mathrm{Frob}) + \underbrace{\widehat{\mathrm{Frob}} \circ \mathrm{Frob}}$

This is $\deg(\mathrm{Frob}) = q$.
Note $|\mathrm{Ker}(\mathrm{Frob})| = 1$.
Here we see the technicality: inseparability

$= 1 - \underbrace{\mathrm{Tr}(\mathrm{Frob})} + q$

the "trace of Frobenius".

Easy parts: * Show $|\mathrm{Tr}(\mathrm{Frob})| \leq 2\sqrt{q}$ (play with above)
* Get a complete proof of the Weil conjectures.

Harder parts: Explain what $\hat{\phi}$ is and why it exists (easier over $\mathbb{C}$)
Understand the complications regarding degree.

23.3. The dual isogeny.

Theorem. Let $\phi : E_1 \to E_2$ be an isogeny of degree m. Then there exists a unique isogeny $\hat{\phi} : E_2 \to E_1$, also of degree m, with

$$\hat{\phi} \circ \phi = [m] \quad \text{(multiplication by } m\text{)}.$$

Properties: Let $\phi : E_1 \to E_2$ be an isogeny. Then,

(1) $\phi \circ \hat{\phi} = [m]$ also (this one on E_2)

(2) For any isogeny $\lambda : E_2 \to E_3$,

$$\widehat{\lambda \circ \phi} = \hat{\phi} \circ \hat{\lambda}.$$

(3) For any isogeny $\psi : E_1 \to E_2$,

$$\widehat{\phi + \psi} = \hat{\phi} + \hat{\psi}.$$

(4) For any $m \in \mathbb{Z}$,

$$\widehat{[m]} = [m], \quad \deg [m] = m^2.$$

(5) $$\hat{\hat{\phi}} = \phi.$$

This is especially interesting if $E_1 = E_2$, the set of isogenies forms a ring, the endomorphism ring $\mathrm{End}(E)$.

Duality gives this ring some additional structure.

23.4.

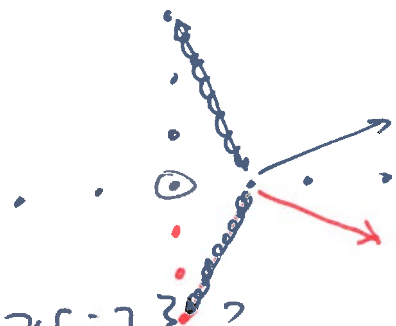
Example. Consider $E: y^2 = x^3 - x \quad / \mathbb{C}$.
Then this is isomorphic to $\mathbb{C}/\mathbb{Z}[i]$ as a complex manifold and as an abelian group.

Recall, $\operatorname{End}(E) \cong \{\alpha \in \mathbb{Z}[i] : \alpha\mathbb{Z}[i] \subseteq \mathbb{Z}[i]\}$

$$= \mathbb{Z}[i].$$

The map $z \longrightarrow \alpha z$ is the isogeny.

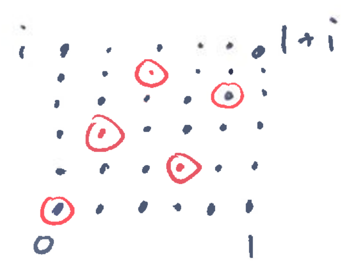
Suppose $\alpha =$ (mult. by $2+i$)



What is the kernel?
What is $\{z \in \mathbb{C} : (2+i)z \in \mathbb{Z}[i]\}$?

A necessary condition is that $5z \in \mathbb{Z}[i]$,
because $2-i$ also maps $\mathbb{Z}[i] \to \mathbb{Z}[i]$.

Indeed, the kernel is generated by $\dfrac{2-i}{5}$.



We have unique factorization of ideals in $\mathbb{Z}[i]$

$$(5) = (2+i)(2-i)$$

and ideals are invertible in a Dedekind domain

$$\{z \in \mathbb{Z}[i] : z(2+i) \in (5)\}$$
$$= \{z \in \mathbb{Z}[i] : z \in (5)(2+i)^{-1} = (2-i)\}, \text{ and}$$

23.5

$\{z \in \mathbb{Z}[i] : z(2+i) \in (1)\}$

$= \{z \in \mathbb{Z}[i] : z \in (2+i)^{-1} = \frac{(2-i)}{(5)} = \{\frac{1}{5}(a+bi)(2-i) : a,b \in \mathbb{Z}\}$.

So if $2+i$ is the isogeny, what is its dual?
$2-i$. By everything we've described.

So $\mathrm{End}(E) = \mathbb{Z}[i]$ has: multiplication (composition)
addition (group law)
complex conjugation (duality).

Theorem. Let E be an elliptic curve over ~~a~~ field K.
(Here K is any perfect field – every alg. extension is separable – so $\mathbb{Q}, \mathbb{Q}_p, \mathbb{F}_p, \mathbb{R}, \mathbb{C}$, any alg. extension
main exception: $\mathbb{F}_q(t)$.)

Then $\mathrm{End}(E)$ is one of the following:

(1) $\mathrm{End}(E) \cong \mathbb{Z}$. (e.g. only multiplication by n)

(2) $\mathrm{End}(E)$ is an order in an imaginary quadratic field.
(i.e. $\mathrm{End}(E) \otimes_{\mathbb{Z}} \mathbb{Q}$ is an IQF.)

(3) $\mathrm{End}(E)$ is an order in a quaternion algebra $/\mathbb{Q}$.

i.e. $\mathbb{Q} + \mathbb{Q}\alpha + \mathbb{Q}\beta + \mathbb{Q}\alpha\beta$:
$\alpha^2, \beta^2 \in \mathbb{Q}$, $\alpha^2 < 0$, $\beta^2 < 0$, $\beta\alpha = -\alpha\beta$.

Need to use duality to get this structure.