16.3 = 17.1.

Today: Arithmetic geometry over finite fields.

Sample question. Let V be any algebraic variety. what is $\# V(\mathbb{F})$ for a finite field F?

Example. Let $V = V(x^2 + y^2 - 1)$. Count $\# V(\mathbb{F}_p)$, i.e.

$$\#\{(x,y) \in \mathbb{F}_p^2 : x^2 + y^2 - 1 = 0\}.$$

Side note for experts. V isn't something we've properly defined. We'll keep it that way.

p	2	3	5	7	11	13	17	19	23	29
$\# V(\mathbb{F}_p)$	2	4	4	8	12	12	16	20	24	28

Example. Let $V = V(y^2 - (x^3 - 1))$. Count $\# V(\mathbb{F}_p)$.

p	2	3	5	7	11	13	17	19	23	29	...
$\# V(\mathbb{F}_p)$	2	3	5	3	11	11	17	27	23	29	

Example. Let $V = V(x^2 - y^2) \subseteq \mathbb{A}^2$.

p	2	3	5	7	11	13	17	19
$\# V(\mathbb{F}_p)$	2	5	9	13	21	25	33	37

16.~~5~~ = 17.2.

The last one we can explain.

If $p = 2$ then $(x^2 - y^2) = (x-y)^2$

and so $V(x^2 - y^2)(\mathbb{F}_p) = V(x-y)(\mathbb{F}_p)$.

Otherwise, $x^2 - y^2 = (x-y)(x+y)$

so $x = \pm y$. If $y = 0$, get one point.

Otherwise, $y \neq -y$ so get two points.

So $2p - 1$ total.

Moral. If V is reducible, can understand in terms of its components.

Review of finite fields.

There exists a finite field of order n if and only if $n = p^a$ for some prime p and positive integer a.

If $n = p$, $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$

If $n = p^a$ for $a \geq 2$, $\mathbb{F}_{p^a} = \mathbb{F}_p[x]/f(x)$

where f is any monic irreducible over $\mathbb{F}_p$ of degree a.

It is unique up to isomorphism, it is Galois over $\mathbb{F}_p$, and $\mathrm{Gal}(\mathbb{F}_{p^a}/\mathbb{F}_p)$ is cyclic, generated by the Frobenius automorphism

$$x \longrightarrow x^p.$$

Recall: $(x+y)^p = x^p + y^p$ in characteristic p!

Same goes for $\mathrm{Gal}(\mathbb{F}_{q^a}/\mathbb{F}_q)$.

16.4 = 17.3.

Example. (Gauss)

Let $V = V(x^3 + y^3 + z^3) \subseteq \mathbb{P}^2$ (not $\mathbb{A}^2$)

If $p \not\equiv 1 \pmod 3$ then $\# V(\mathbb{F}_p) = p + 1$.

If $p \equiv 1 \pmod 3$ then there are integers A, B

with $4p = A^2 + 27B^2$.

A and B are unique up to changing their signs.

If we choose the sign of A s.t. $A \equiv 1 \pmod 3$,

$$\# V(\mathbb{F}_p) = p + 1 + A.$$

Example. Let $V = V(x^2 + y^2 - z^2) \subseteq \mathbb{P}^2$.

Projectivization of first example.

If $p \neq 2$ (and maybe even if $p = 2$? I didn't check) I think so actually

the usual "stereographic projection" method yields an isomorphism $V \xrightarrow{\sim} \mathbb{P}^1$.

This induces a bijection $V(\mathbb{F}_p) \xrightarrow{\sim} \mathbb{P}^1(\mathbb{F}_p)$ for every p.

So $\# V(\mathbb{F}_p) = p + 1$.

Consider again its affine patch $V_1 = V(x^2 + y^2 - 1) \subseteq \mathbb{A}^2$.

Then $\# V(\mathbb{F}_p) = \# V_1(\mathbb{F}_p) + \#\{(x, y) \in \mathbb{P}^2(\mathbb{F}_p) : x^2 + y^2 - 0 = 0\}$.

Estimate the right. x and y are nonzero.

By scaling $y = 1$. So $\#\{x \in \mathbb{F}_p : x^2 + 1 = 0\}$

$= 1 + \left(\frac{-1}{p}\right)$.

17.4.

Therefore $\# V_1(\mathbb{F}_p) = (p+1) - \left(1 + \left(\frac{-1}{p}\right)\right)$

$$= p - \left(\frac{-1}{p}\right)$$

$$= \begin{cases} p-1 & \text{if } p \equiv 1 \pmod 4 \\ p+1 & \text{if } p \equiv 3 \pmod 4 \end{cases}.$$

Example. Distribution of quadratic residues.

If x is a quadratic residue $(\bmod\ p)$, is $x+1$ more or less likely to be?

	1	2	3	4	5	6	7	8	9	10
$p = 11$:	O	X	O	O	O	X	X	X	O	X

$$\#\left\{x \in \mathbb{F}_{11} : \left(\frac{x}{p}\right) = \left(\frac{x+1}{p}\right) = 1\right\} = 2.$$

We have $\#\left\{x \in \mathbb{F}_p : \left(\frac{x}{p}\right) = \left(\frac{x+1}{p}\right) = 1\right\}$

$$= \frac{1}{2}\#\left\{y \in \mathbb{F}_p - \{0\} : y^2 + 1 \in \mathbb{F}_p^{2} - \{0\}\right\}$$

$$= \frac{1}{4}\#\left\{y, z \in \mathbb{F}_p - \{0\} : y^2 + 1 = z^2\right\}$$

Now, if $y = 0 \Rightarrow$ get two points. (as long as $p \neq 2$)

if $z = 0 \Rightarrow$ get $1 + \left(\frac{-1}{p}\right)$ points.

So, get $\frac{1}{4}\left(\#\{y, z \in \mathbb{F}_p : y^2 + 1 = z^2\} - 3 - \left(\frac{-1}{p}\right)\right)$

17.5.

Now projectivize it, consider

$$(y:z:w) \in \mathbb{P}^2(\mathbb{F}_p) : \quad y^2 + w^2 = z^2$$

which introduces two more points with $w=0$.

Get

$$\frac{1}{4}\left(\#\{(y:z:w) \in \mathbb{P}^2(\mathbb{F}_p) : y^2 + w^2 = z^2\} - 5 - \left(\frac{-1}{p}\right)\right)$$

$$= \frac{1}{4}\left(p+1 - 5 - \left(\frac{-1}{p}\right)\right)$$

$$= \frac{1}{4}\left(p - 4 - \left(\frac{-1}{p}\right)\right).$$

So take $\frac{p}{4}$, round off to the nearest integer, subtract 1.

Note. This proved (somehow!) that $\left(\frac{-1}{p}\right) = \begin{cases} 1 & \text{if } p \equiv 1 \pmod 4 \\ -1 & \text{if } p \equiv 3 \pmod 4 \end{cases}$.

18.1. The Weil Conjectures.

Let $V/\mathbb{F}_q$ be a projective variety, and define the zeta function

$$Z(V/\mathbb{F}_q; T) = \exp\left(\sum_{n=1}^{\infty} \# V(\mathbb{F}_{q^n}) \frac{T^n}{n}\right).$$

Regard it as a formal power series in T.

Example. Let $V = \mathbb{P}^1/\mathbb{F}_p$ Then $\# V(\mathbb{F}_{p^n}) = p^n + 1$ for all n.

$$Z(\mathbb{P}^1/\mathbb{F}_p; T) = \exp\left(\sum_{n=1}^{\infty} (p^n + 1) \frac{T^n}{n}\right)$$

$$= \exp\left(\sum_{n=1}^{\infty} \frac{(pT)^n}{n}\right) \cdot \exp\left(\sum_{n=1}^{\infty} \frac{T^n}{n}\right).$$

Recall that $-\log(1-x) = \sum_{n=1}^{\infty} \frac{x^n}{n}$, so

$$Z(\mathbb{P}^1/\mathbb{F}_p; T) = \exp(-\log(1-pT)) \cdot \exp(-\log(1-T))$$

$$= \frac{1}{(1-pT)(1-T)}.$$

Theorem. (Hasse)

Let V be an $EC/\mathbb{F}_q$. Then

$$\# V(\mathbb{F}_{q^n}) = 1 - \alpha^n - \bar{\alpha}^n + q^n$$

for some complex numbers $\alpha, \bar{\alpha}$ with $\alpha\bar{\alpha} = q$.

18.2. Then

$$Z(V/\mathbb{F}_q;T) = \exp\left(\sum_{n=1}^{\infty}(1-\alpha^n-\bar{\alpha}^n+q^n)\frac{T^n}{n}\right)$$

$$= \frac{(1-\alpha T)(1-\bar{\alpha}T)}{(1-qT)(1-T)} = \frac{1-(\alpha+\bar{\alpha})T+qT^2}{(1-qT)(1-T)}$$

Theorem. (The Weil Conjectures: Dwork '60, Deligne '73)

Let $V/\mathbb{F}_q$ be an (irreducible) smooth projective variety of dimension n, and let

$$Z(V/\mathbb{F}_q;T) = \exp\left(\sum_{n=1}^{\infty}\#V(\mathbb{F}_{q^n})\frac{T^n}{n}\right)$$

be its zeta function. Then:

(1. Rationality) $Z(V/\mathbb{F}_q;T) \in \mathbb{Q}(T)$.

(2. Functional Equation) There is an integer ε (the Euler characteristic of V) s.t.

$$Z(V/\mathbb{F}_q;q^{-n}T) = \pm q^{n\varepsilon/2}T^{\varepsilon}Z(V/\mathbb{F}_q;T).$$

(3. Riemann Hypothesis) There is a factorization

$$Z(V/\mathbb{F}_q;T) = \frac{P_1(T)\cdots P_{2n-1}(T)}{P_0(T)P_2(T)\cdots P_{2n}(T)}$$

and ~~for each~~ $P_0(T) = 1-T$

$P_{2n}(T) = 1-q^nT$

for each i with $1 \le i \le 2n-1$, $P_i(T) = \prod_j (1-\alpha_{ij}T)$

$|\alpha_{ij}| = q^{i/2}$.

So
$$Z(E/\mathbb{F}_q;T) = \exp\left(\sum_{n=1}^{\infty} \#E(\mathbb{F}_{q^n})\frac{T^n}{n}\right)$$

$$= \exp\left(\sum_{n=1}^{\infty}\sum_{d\mid n} d\,\#\left\{\begin{matrix}\text{closed pts. of}\\ \deg d\end{matrix}\right\}\frac{T^n}{n}\right)$$

$$= \exp\left(\sum_{d=1}^{\infty} d\,\#\{\text{CP deg } d\}\sum_{\substack{n=1\\ d\mid n}}^{\infty}\frac{T^n}{n}\right)$$

$$= \exp\left(\sum_{d=1}^{\infty} \#\{\text{CP deg } d\}\sum_{m=1}^{\infty}\frac{T^{dm}}{dm}\right)$$

$$= \exp\left(\sum_{d=1}^{\infty} \#\{\text{CP deg } d\}\cdot -\log(1-T^{d})\right)$$

$$= \exp\left(\sum_{x\in|E|} -\log(1-T^{\deg x})\right)$$

$$= \prod_{x\in|E|}(1-T^{\deg x})^{-1}.$$

Remark. You can also prove the proposition by taking the operator $f \to -T\frac{f'}{f}$ on both sides. A bit quicker.

Now, recall that an effective divisor on a curve is a nonnegative formal sum of closed points.

If we write $\deg(P_1+\cdots+P_n) = \deg(P_1)+\cdots+\deg(P_n)$ then

$$\prod_{x\in|E|}(1-T^{\deg x})^{-1} = \prod_{x\in|E|}(1+T^{\deg x}+T^{2\deg x}+\cdots)$$
$$= \sum_{\substack{D\\ \text{eff. divisor on } E}} T^{\deg(D)}. \quad \left(= \sum_D q^{-s\deg D}\right)$$

Why "Riemann hypothesis"?

Write $T = q^{-s}$, then says that

$$Z(T) = 0 \longleftrightarrow 1 - \alpha_{ij} T = 0 \text{ for some } \alpha_{ij} \quad (\text{recall: } |\alpha_{ij}| = q^{1/2},$$

so $T = q^{-s}$ with $\mathrm{Re}(s) = 1/2$.

Proposition. RH is true for $\mathbb{P}^1$.

Proof. $\dfrac{1}{(1-qT)(1-T)}$ is never zero.

We'll focus on the EC case, and see one more perspective.

Def. Let $E/\mathbb{F}_q$ be an elliptic curve.
A closed point of E is the Galois orbit of a point $x_0 \in E(\overline{\mathbb{F}}_q)$. Its degree $\deg(x)$ is the (finite!) cardinality of the orbit. Its norm $N(x)$ is $q^{\deg(x)}$.

Proposition. We have

$$Z(E/\mathbb{F}_q;T) = \prod_{\substack{x \in |E| \\ \text{all closed pts. of } E}} \left(1 - T^{\deg(x)}\right)^{-1}.$$

Proof. Note that we have

$$\# E(\mathbb{F}_{q^n}) = \sum_{d \mid n} \#\text{ of closed points of degree } d,$$

because

$$\mathbb{F}_{q^a} \subseteq \mathbb{F}_{q^b} \Longleftrightarrow a \mid b.$$

18.5 This exists in analogy with

$\operatorname{Spec}(\mathbb{Z}) = \{\text{all prime ideals in } \mathbb{Z}\}$

a closed point is any other than (0)

$\longleftrightarrow$ a prime integer p.

A nonnegative formal sum of closed points corresponds to an integer. If $n^{-s} \longleftrightarrow q^{-s \deg D}$, we get an analogue of

$$\prod_p (1 - p^{-s})^{-1} = \sum_{n=1}^{\infty} n^{-s} = \zeta(s).$$

Our goal. Sketch three proofs for elliptic curves.

(1) Stepanov's method.
Prove that $\#(y^2 - f(x) = 0)(\mathbb{F}_q) \sim q$ by elementary methods.
No AG required!

(2) Using the Riemann-Roch theorem.

Stepanov's method. (Reference: Iwaniec-Kowalski, 11.6)

Theorem. Given a hyperelliptic curve over $\mathbb{F}_q$

$$C_f : y^2 = f(x)$$

where $f(x)$ is of degree ≥ 3, not a square in $\overline{\mathbb{F}_q}[x]$.

Then, if $q > 4m^2$, we have

$$\left| \# C_f(\mathbb{F}_q) - q \right| < 8m\sqrt{q}.$$

Proof is completely elementary (no AG!) but not easy.

Can prove $\# C_f(\mathbb{F}_q) < q + 8m\sqrt{q}$ "directly"

get the lower bound by a trick.

Let $N = \# C_f(\mathbb{F}_q)$

$= N_0 + 2N_1$

N_0: # of points $(x, 0) \in C_f(\mathbb{F}_q)$
$= \#$ of distinct roots of f.

N_1: # of $x \in \mathbb{F}_q$ with $f(x)$ a (nonzero) square in $\mathbb{F}_q$.

Also write

$N_1 = \#$ of $x \in \mathbb{F}_q$ with $f(x)^{\frac{q-1}{2}} = 1$.

Writing $g := f^{\frac{q-1}{2}}$, want to estimate

$$N_1 = |\{x \in \mathbb{F}_q : g(x) = 1\}|$$

Write

$$S_1 = \{x \in \mathbb{F}_q : f(x) = 0 \text{ or } g(x) = 1\}$$

and to generalize,

$$S_a = \{x \in \mathbb{F}_q : f(x) = 0 \text{ or } g(x) = a\}.$$

19.2.

Claim 1. We have, for $a \in \{1, -1\}$,

$$|S_a| \le \frac{q-1}{2} + 4m\sqrt{q}.$$

Suppose you accept Claim 1. We'll show how this implies Stepanov. For the upper bound we have

$$N = N_0 + 2N_1 \le 2(N_0 + N_1) = 2|S_a|$$

$$\le q + 8m\sqrt{q}.$$

Trick for the lower bound.

We have $X^q - X = X(X^{\frac{q-1}{2}} - 1)(X^{\frac{q-1}{2}} + 1)$, so for all $x \in \mathbb{F}_q$,

$$0 = f(x)^q - f(x) = f(x)(g(x) - 1)(g(x) + 1)$$

and so $q = N_0 + N_1 + \underbrace{N_{-1}}_{\#\{x \in \mathbb{F}_q : g(x) = -1\}}$

and $N_0 + N_{-1} = |S_{-1}| \le \frac{q-1}{2} + 4m\sqrt{q}$

So $N_1 = q - N_0 - N_{-1} \ge q - \frac{q-1}{2} - 4m\sqrt{q}$

$$\ge \frac{q}{2} - 4m\sqrt{q}$$

$$N = N_0 + 2N_1 \ge 2N_1 \ge q - 8m\sqrt{q}.$$

19.3.

Claim 2. We have for $a \in \{-1, 1\}$, $q > 8m$, and any integer $\ell \in (m, \frac{q}{8}]$: There exists a polynomial $r \in \mathbb{F}_q[x]$ of degree

$$\deg(r) < \frac{q-1}{2}\ell + 2m\ell(\ell-1) + mq$$

with ~~a~~ zero of order at least ℓ at all points $x \in S_a$.

Proof of Claim 1. We have

$$\ell |S_a| \le \deg(r) \le \frac{q-1}{2}\ell + 2m\ell(\ell-1) + mq$$

So $|S_a| \le \frac{q-1}{2} + 2m(\ell-1) + \frac{mq}{\ell}$

Choose $\ell = 1 + \lfloor \frac{\sqrt{q}}{2} \rfloor$ (and hence demand $1 + \frac{\sqrt{q}}{2} > m$

$\sqrt{q} > 2m - 2$

enough if $q > 4m^2$.)

Then $|S_a| \le \frac{q-1}{2} + 2m \cdot \frac{\sqrt{q}}{2} + 2m\sqrt{q} = \frac{q-1}{2} + 4m\sqrt{q}$.

Claim 2 is the heart of the matter!

How to identify zeroes of order $\ge \ell$?

In ordinary calculus,

$f(x)$ has a zero of order ℓ $\Longleftrightarrow$ $f^{(i)}(x) = 0$ for all $i < \ell$.

But here, for example, $\frac{d^i}{dx^i}(x^p) = 0$ for all i.

We tweak to get a "characteristic p derivative".

19.4.

Hasse Derivatives. Let k be any field (char p or otherwise).

For each $k \geq 0$, the kth Hasse derivative is the linear operator $E^k : k[X] \to k[X]$ defined by

$$E^k X^n = \binom{n}{k} X^{n-k},$$

and extended to all of $k[X]$ by linearity.

So, for example, $E^p X^p = 1$ which is not zero.

Lemma. For all $f, g \in k[X]$ we have

(1) $$E^k(fg) = \sum_{j=0}^{k} (E^j f)(E^{k-j} g);$$

for all $f_1, \ldots, f_r \in k[X]$ we have

(2) $$E^k(f_1 \cdots f_r) = \sum_{j_1+\cdots+j_r=k} (E^{j_1} f_1) \cdots (E^{j_r} f_r).$$

Proof. (2) follows by (1) and induction. To prove (1) it is enough by linearity to assume $f = X^m$, $g = X^n$, and prove

$$E^k(X^{m+n}) = \sum_{j=0}^{k} E^j X^m \cdot E^{k-j} X^n, \text{ i.e.}$$

$$\binom{m+n}{k} X^{m+n-k} = \sum_{j=0}^{k} \binom{m}{j} X^{m-j} \binom{n}{k-j} X^{n-(k-j)}$$

The powers of X is equal, so this is the combinatorial identity

$$\binom{m+n}{k} = \sum_{j=0}^{k} \binom{m}{j}\binom{n}{k-j}.$$

19.5.

<u>Lemma</u>. For all $k, r \geq 0$, all $a \in K$,

$$E^k (X-a)^r = \binom{r}{k} (X-a)^{r-k}.$$

No, you can't use the chain rule. ~~Ex: have a zero of~~

<u>Proof</u>. Apply (2) of the previous lemma.

$$E^k (X-a)^r = \sum_{j_1 + \cdots + j_r = k} E^{j_1}(X-a) \cdots E^{j_r}(X-a)$$

and only the terms with all $j_i \in \{0,1\}$ survive.
Each of these terms is $(X-a)^{r-k}$ and there are $\binom{r}{k}$ of them.

<u>Lemma</u>. For all $k, r \geq 0$ with $k \leq r$, all $f, g \in K[X]$,

$$E^k (f g^r) = h g^{r-k}$$

with h some poly w/ degree $\leq \deg(f) + k \deg(g) - k$.

[Same idea in proof. Left as an exercise.]
[Think: a basic property of ordinary derivatives.]

(skip proof)
<u>Technical Lemma</u>. Let $K = \mathbb{F}_q$ of char p now, $h \in \mathbb{F}_q[X, Y]$, $r = h(X, X^q) \in \mathbb{F}_q[X]$. Then for all $k < q$

$$E^k r = \underbrace{(E^k_X h)}_{\text{kth Hasse derivative w.r.t. } X}(X, X^q).$$

(Sketch)
<u>Proof</u>. By linearity assume $h = X^n Y^m$, use $\binom{mq}{j} = 0$ for $0 < j < q$ in char p.

20.1. Stepanov continued.

* Review statement
[* Review Claim 2 (p. 19.3). Do before proof
* Review def. of Hasse derivs
* Prove lemma at top of p. 19.5.

Lemma. Let $f \in K[X]$, $a \in K$. Suppose $(E^k f)(a) = 0$ for all $k < l$.

Then f has a zero of order $\geq l$ at a, i.e. f is divisible by $(X-a)^l$.

Proof. Let $f = \sum_{0 \leq i \leq d} q_i (X-a)^i$ be the "Taylor expansion" of f around a.

(Exercise. Such exists.)

Then by lemma, $E^k f = \sum_{k \leq i \leq d} q_i \binom{i}{k} (X-a)^{i-k}$.

By hypothesis $(E^k f)(a) = 0$ for $k < l$, so $q_k = 0$ (look at $i = k$ term).

[State central proposition now.]

Write $$r = f^l \sum_{0 \leq j < J} (r_j + s_j g) X^{jq},$$

where $r_j, s_j \in \mathbb{F}_q[X]$ to be constructed have degree $\leq \frac{q-1}{2} - m$.

Then

$$\deg(r) \leq \underset{\deg(f)}{l \cdot m} + \left(\frac{q-1}{2} - m\right) + \underbrace{\frac{q-1}{2} \cdot m}_{g = f^{\frac{q-1}{2}}} + Jq \leq \underbrace{(J+m)q}_{\text{Use } l \leq \frac{q}{8}}.$$

20.2. Lemma. We have $r=0$ if and only if all the r_j and s_j are 0.

Proof. "If" is obvious. Assume $r=0$, not all r_j, s_j are.

WLOG $f(0) \neq 0$. (Change variables $X \to X+a$ if necessary.)

Choose k minimal s.t. some r_k or s_k is nonzero.

Then

$$0 = f^{\ell} \sum_{k \le j < J} (r_j + s_j g) X^{jq}$$

$$= \sum_{k \le j < J} (r_j + s_j g) X^{(j-k)q} \qquad (\text{since } X^{kq} f^{\ell} \neq 0)$$

$$= \underbrace{\left(\sum_{k \le j < J} r_j X^{(j-k)q} \right)}_{\text{write } h_0} + \underbrace{\left(\sum_{k \le j < J} s_j X^{(j-k)q} \right)}_{\text{write } h_1} g.$$

So $h_0 = -h_1 g \Rightarrow h_0^2 f = h_1^2 g^2 f = h_1^2 f^{\frac{\ell-1}{2}\cdot 2} \cdot f$

$$= h_1^2 f^q$$

$$= h_1^2 f(X)^q$$

$$= h_1^2 f(X^q)$$

$$\equiv h_1^2 f(0) \pmod{X^q}.$$

So: $\boxed{r_k^2 f \equiv s_k^2 f(0) \pmod{X^q}.}$

But $\deg(r_k^2 f) \le 2\deg(r_k) + m \le 2\left(\frac{q-1}{2} - m\right) + m < q$

$\deg(s_k^2 f(0)) \le 2\deg(s_k) < q$

and so $r_k^2 f = s_k^2 f(0)$ and f is a square in $\mathbb{F}_{q^2}[X]$.

Contradicts hypothesis!

Lemma. Let $k \le l$. We have

$$E^k r = f^{l-k} \sum_{0 \le j < J} \left(r_j^{(k)} + s_j^{(k)} g\right) X^{jq}$$

for some polynomials $r_j^{(k)}, s_j^{(k)}$ of degree $\le \frac{q-1}{2} - m + k(m-1)$.

Proof. Ugly hack and slash. Omitted.

The conclusion. Want r to have zeroes of order $\ge l$ at every point of S_a. If $f(x) = 0$ true by construction. So let $x \in S_a$ with $f(x) \ne 0$.

By previous lemma

$$(E^k r)(x) = f(x)^{l-k} \, \sigma^{(k)}(x)$$

with $\sigma^{(k)}(X) = \sum_{0 \le j < J} \left(r_j^{(k)} + a s_j^{(k)}\right) X^j$.

note: $g(x) = a$

Note: not X^{jq}. use $x^q = x$ for $x \in \mathbb{F}_q$.

Impose the conditions $\sigma^{(k)}(X) = 0$ for $k < l$.

Unknowns: coefficients of the polys r_j, s_j.

~~Using the degree bound in the lemma,~~ These equations are linear in these unknowns.

~~# unknowns~~ $\cancel{= \sum_{0 \le j < J}}$

20.4.

Unknowns : coeffs of the r_j and s_j.

There are $2J \cdot \left(\frac{q-1}{2} - m\right)$ of them.

Equations.

$$\sum_{k<\ell} \deg\left(r^{(k)}\right)$$

$$< \sum_{k<\ell} \left(\frac{q-1}{2} - m + k(m-1) + J\right)$$

$$\leq \ell\left(\frac{q-1}{2} - m + J\right) + \frac{\ell(\ell-1)}{2} \cdot (m-1).$$

Suppose there are ~~more~~ fewer equations than unknowns.
(Choose J big.)

This is guaranteed if

$$J = \frac{\ell}{q}\left(\frac{q-1}{2} + 2m(\ell-1)\right)$$

Then there is a nontrivial solution.

Thus we're done: $(E^k r)(x) = 0$ for all $k < \ell$
all $x \in S_a$

So r has zeroes of order $\geq \ell$ at all $x \in S_a$ as required. QED.