Examples (cont’d): Function fields in one variable... as algebraic parallels to $\mathbb{Z}$ and $\mathbb{Q}$.

**Theorem:** All finite field extensions of $\mathbb{C}((X - z))$ are by adjoining solutions to $Y^e = X - z$ for $e = 2, 3, 4, \ldots$ [Done]

Thus,

$$\text{Gal}(\overline{\mathbb{C}((X))/\mathbb{C}((X))}) = \lim_d \mathbb{Z}/d = \hat{\mathbb{Z}} \approx \prod_p \mathbb{Z}_p$$

Few explicit parametrizations of algebraic closures of fields are known: not $\overline{\mathbb{Q}}$, for sure. But we do also know

$$\text{Gal}(\overline{\mathbb{F}_q}/\mathbb{F}_q) = \lim_d \mathbb{Z}/d = \hat{\mathbb{Z}} \approx \prod_p \mathbb{Z}_p$$
In anticipation: **Newton polygons over** $\mathbb{Q}_p$

This is the assertion for $\mathbb{Z}_p[T]$ corresponding to $\mathbb{C}[[X]][T]$ above.

The **Newton polygon** of a polynomial $f(T) = T^n + a_{n-1}T^{n-1} + \ldots + a_0 \in \mathbb{Z}_p[T]$ is the (downward) convex hull of the points

$$(0, 0), (1, \text{ord}_p a_{n-1}), (2, \text{ord}_p a_{n-2}), \ldots (n, \text{ord}_p a_0)$$

When we extend $\text{ord}_p(p^n \cdot \frac{a}{b}) = n$ to algebraic extensions of $\mathbb{Q}_p$, we will prove that the **slopes** of the line segments on the Newton polygon are the **ords**, with multiplicities, of the zeros.

The extreme case that $\text{ord}_p a_0 = 1$ is **Eisenstein’s criterion**.

This device is one of few human-accessible computational means.

We will get to this...
Returning to *finite* scalars in place of \( \mathbb{C} \)... a key point is the finiteness of residue fields \( \mathfrak{o}/ \mathfrak{p} \).

**Infinitude of primes:** Because the algebraic closure of \( \mathbb{F}_q \) is of infinite degree over \( \mathbb{F}_q \), by *separability* there are single elements \( \alpha \) of arbitrarily large degree, whose minimal polynomials in \( \mathbb{F}_q[X] \) give prime elements of arbitrarily large degree, thus, *infinitely-many*.

*Also,* we can mimic Euclid’s proof. Use the fact that \( \mathbb{F}_q[X] \) is a PID. Given any finite collection \( P_1, \ldots, P_n \) of monic irreducibles in \( \mathbb{F}_q[X] \), the element \( N = X \cdot P_1 \ldots P_n + 1 \) is of positive degree, so has *some* irreducible factor, but is not divisible by any \( P_j \).  

One should contemplate what it would take to prove an analogue of *Dirichlet’s Theorem* on primes in arithmetic progressions.
The finiteness of residue fields allows definition of the \textit{zeta function} of \( \mathfrak{o} = \mathbb{F}_q[X] \):

\[
Z(s) = \sum_{0 \neq \mathfrak{a} \text{ ideal } \subseteq \mathbb{F}_p[X]} \frac{1}{(N\mathfrak{a})^s} = \sum_{0 \neq \mathfrak{a} \text{ ideal } \subseteq \mathbb{F}_p[X]} \frac{1}{(\#\mathbb{F}_p[X]/\mathfrak{a})^s} = \sum_{\text{monic } f} \frac{1}{(\#\mathbb{F}_p[X]/(f))^s} = \sum_{\text{monic } f} \frac{1}{(q^{\deg f})^s} = \sum_{\text{degrees } d} \frac{\#\{\text{monic } f : \deg f = d\}}{q^{ds}} = \sum_{\text{degrees } d} \frac{q^d}{q^{ds}} = \frac{1}{1 - \frac{1}{q^{s-1}}}
\]
Since $\mathbb{F}_q[X]$ is a PID, there is an Euler product

$$Z(s) = \prod_{0 \neq p \text{ prime}} \frac{1}{1 - (Np)^{-s}}$$

$$= \prod_{\text{monic irred } f} \frac{1}{1 - q^{-s \cdot \deg f}}$$

$$= \prod_d \left( \frac{1}{1 - q^{-sd}} \right)^{\# \text{monic irred } f \ \deg = d}$$

convergent for $\Re(s) > 1$. Observe that

$$\# \text{irred monics } \deg d = \frac{\# \text{ elements degree } d \text{ over } \mathbb{F}_q}{\# \text{each Galois conjugacy class}}$$

$$= \frac{1}{d} \left( q^d - \sum_{\text{prime } p | d} q^{d/p} + \sum_{\text{distinct } p_1, p_2 | d} q^{d/p_1p_2} - \sum_{\text{distinct } p_1, p_2, p_3 | d} q^{d/p_1p_2p_3} + \ldots \right)$$

The fact that $Z(s) = 1/(1 - q^{1-s})$ is not obvious from the Euler factorization.
Example: in $\mathbb{F}_3[x]$, monic irreducibles of low degrees are

$$x, \ x + 1, \ x + 2$$

(3 (irred) monic linear)

$$x^2 + 1, \ x^2 + 2x + 2, \ x^2 - 2x + 2$$

$$(\frac{3^2-3}{2} = 3 \text{ irred monic quadratics})$$

$$x^3 - x + 1, \ x^3 - x + 2, \ldots$$

(all $x^3 - a$’s are reducible!?!)

$$(\frac{3^3-3}{3} = 8 \text{ irred monic cubics})$$

$$x^4 - 2x + 1, \ldots$$

(all $x^4 - a$’s are reducible!?!)

$$(\frac{3^4-3^2}{4} = 18 \text{ irred monic quartics})$$

$$???$$

(all $x^5 - a$’s are reducible!?!)

$$(\frac{3^5-3}{5} = 48 \text{ irred monic quintics})$$

No simple conceptual argument, but some reusable tricks... :}
Since $\mathbb{F}_3^\times$ is a cyclic 2-group, there is no 4$^{th}$ root of unity, so the 4$^{th}$ cyclotomic polynomial $x^2 + 1$ is irreducible.

Then $(x + j)^2 + 1$ is irreducible for $j = 1, 2$. This happens to give all 3 irreducible monic quadratics.

Since $x^3 - a = (x - a)^3$ for $a \in \mathbb{F}_3$, none of these cubics is irreducible.

The two cubics $x^3 - x + a$ with $a \neq 0$ are Artin-Schreier polynomials over $\mathbb{F}_3$. Since $\alpha^3 - \alpha = 0$ for $\alpha \in \mathbb{F}_3$, these have no linear factors, so are irreducible. With $j \in \mathbb{F}_3$, $x \to x + j$ leaves these unchanged!

No quartic $x^4 - a \in \mathbb{F}_3[x]$ is irreducible: $\mathbb{F}_3^\times$ is cyclic of order $3^4 - 1 = 80 = 2^4 \cdot 5$, so every $a \in \mathbb{F}_3^\times$ is an 8$^{th}$ power.

Since $(3^2 - 1)/4 = 2$, fourth powers of $\alpha \in \mathbb{F}_3^\times$ have order 2, so are in $\mathbb{F}_3^\times$. Thus, $\alpha^4 \neq a\alpha + b$ for non-zero $a, b \in \mathbb{F}_3$. Thus, the four polynomials $x^4 - ax - b$ with non-zero $a, b \in \mathbb{F}_3$ are irreducible.
Artin-Schreier polynomials:

Taking \( p^{th} \) roots is problematical in characteristic \( p \)... Already the quadratic formula fails in characteristic 2. A root of \( x^2 + x + 1 = 0 \) in \( \mathbb{F}_2 \) cannot be expressed in terms of square roots!

Over \( \mathbb{F}_p \) with prime \( p \), the Artin-Schreier polynomials are \( x^p - x + a \), with \( a \in \mathbb{F}_{p}^\times \).

Claim: Artin-Schreier polynomials are irreducible, with Galois group cyclic of order \( p \).

Proof: For a root \( \alpha \in \overline{\mathbb{F}}_p \) of \( x^p - x + a = 0 \),

\[
(\alpha + 1)^p - (\alpha + 1) + a = \alpha^p - \alpha + a = 0
\]

Thus, any field extension containing one root contains all roots. That is, the splitting field is \( \mathbb{F}_p(\alpha) \) for any root \( \alpha \). But the Frobenius automorphism \( \alpha \to \alpha^p \) generates the Galois group, whatever it is, and \( \alpha^p = \alpha - a \), which is of order \( p \). Thus, the Galois group is cyclic of order \( p \).
For $\mathfrak{o} = \mathbb{F}_p[x]$, completions are

$x$-adic completion of $\mathfrak{o} = \mathbb{F}_p[[x]]$

$(x + 1)$-adic completion of $\mathfrak{o} = \mathbb{F}_p[[x + 1]]$

$(x^2 + 1)$-adic completion of $\mathfrak{o} = \mathbb{F}_p[[x^2 + 1]][x]$

$$= \{(a_0x + b_0) + (x^2 + 1)(a_1x + b_1) + (x^2 + 1)^2(a_2x + b_2) + \ldots\}$$

Generally, for $P$ irreducible monic

$P$-adic completion of $\mathfrak{o}$

$$= c_0(x) + c_1(x) \cdot P + c_2(x) \cdot P^2 + \ldots \quad (\deg c_j < \deg P)$$

Also, corresponding to the point at infinity and its local ring

$\mathbb{F}_p[[1/x]] \cap \mathbb{F}_p(x)$ inside $\mathbb{F}_p(x)$,

$$\frac{1}{x} - \text{adic completion of } \mathfrak{o} = \mathbb{F}_p[[1/x]]$$
In his 1921 thesis, E. Artin considered hyperelliptic curves over a finite field (of odd characteristic, for simplicity):

\[ y^2 = f(x) \quad \text{(with monic } f(x) \in \mathbb{F}_q[x]) \]

These are the quadratic extensions \( K \) of \( k = \mathbb{F}_q(x) \) other than constant field extensions going from \( \mathbb{F}_q(x) \) to \( \mathbb{F}_{q^2}(x) \). We saw that the integral closure of \( \mathfrak{o} = \mathbb{F}_p[x] \) in \( K \) is \( \mathbb{F}_p[x, y] \).

How do primes in \( \mathfrak{o} = \mathbb{F}_q[X] \) behave in these extensions? The algebra computation can be applied: for \( P \) degree \( d \) monic prime in \( \mathbb{F}_q[x] \), and for \( \mathcal{O} = \mathbb{F}_q[x, y] \), letting \( \alpha \) be the image of \( x \) in \( \mathbb{F}_q[x]/P \approx \mathbb{F}_q^d \),

\[
\mathcal{O}/\langle P \rangle \approx \mathbb{F}_q[x, t]/\langle P, t^2 - f \rangle \approx \mathbb{F}_q^d[t]/\langle t^2 - f(\alpha) \rangle
\]

Thus, apart from the ramified prime \( \langle f(x) \rangle \subset \mathbb{F}_q[x] \), which becomes a square, there are split primes and inert primes:

\[
\begin{cases} 
\mathcal{O}/\langle P \rangle \approx \mathbb{F}_q^d \oplus \mathbb{F}_q^d & \text{and } P\mathcal{O} \approx \mathfrak{p}_1 \cap \mathfrak{p}_2 & \text{(if } f(\alpha) \in (\mathbb{F}_q^d)^\times) \\
\mathcal{O}/\langle P \rangle \approx \mathbb{F}_{q^{2d}} & \text{and } P\mathcal{O} = \text{prime in } \mathcal{O} & \text{(if } f(\alpha) \notin (\mathbb{F}_q^d)^\times) 
\end{cases}
\]
**Example:** for \( y^2 = x^2 + 1 \) over \( \mathbb{F}_3 \),

\[
\mathcal{O}/\langle x \rangle \approx \mathbb{F}_3[x, t]/\langle x, t^2 - x^2 - 1 \rangle \approx \mathbb{F}_3[t]/\langle t^2 - 1 \rangle \approx \mathbb{F}_3 \oplus \mathbb{F}_3
\]

\[
\mathcal{O}/\langle x + 1 \rangle \approx \mathbb{F}_3[x, t]/\langle x + 1, t^2 - x^2 - 1 \rangle \approx \mathbb{F}_3[t]/\langle t^2 - 2 \rangle \approx \mathbb{F}_3^2
\]

\[
\mathcal{O}/\langle x - 1 \rangle \approx \mathbb{F}_3[x, t]/\langle x - 1, t^2 - x^2 - 1 \rangle \approx \mathbb{F}_3[t]/\langle t^2 - 2 \rangle \approx \mathbb{F}_3^2
\]

\[
\mathcal{O}/\langle x^2 + 1 \rangle \approx \mathbb{F}_3[x, t]/\langle x^2 + 1, t^2 - x^2 - 1 \rangle \approx \mathbb{F}_3^2[t]/\langle t^2 \rangle \approx \text{not product}
\]

That is, unsurprisingly, the prime \( x^2 + 1 \) is *ramified*. Ok.

\[
\mathcal{O}/\langle x^2 + 2x + 2 \rangle \approx \mathbb{F}_3[x, t]/\langle x^2 + 2x + 2, t^2 - x^2 - 1 \rangle
\]

\[
\approx \mathbb{F}_3(\alpha)[t]/\langle t^2 - \alpha^2 - 1 \rangle
\]

Is \( \alpha^2 + 1 \) a *square* in \( \mathbb{F}_3(\alpha) \approx \mathbb{F}_3^2 \) where \( \alpha^2 + 2\alpha + 2 = 0 \)? Some brute-force computation?
\[ \mathcal{O}/\langle x^3 - x + 1 \rangle \approx \mathbb{F}_3[x, t]/\langle x^3 - x + 1, t^2 - x^2 - 1 \rangle \]
\[ \approx \mathbb{F}_3(\alpha)[t]/\langle t^2 - \alpha^2 - 1 \rangle \quad \text{(with } \alpha^3 - \alpha + 1 = 0) \]

Is \( \alpha^2 + 1 \) a square in \( \mathbb{F}_3(\alpha) \approx \mathbb{F}_{3^3} \)? More brute-force computation?

Or, ... a clear pattern of whether \( f(\alpha) \) is a square in \( \mathbb{F}_p(\alpha) \)?

\( \mathbb{F}_p(\alpha)^\times \) is cyclic, and Euler’s criterion applies:

\[ f(\alpha) \in \mathbb{F}_p(\alpha)^\times \iff f(\alpha)^{q^{d-1}/2} = 1 \]

What should \textit{quadratic reciprocity} be here? \textit{Why} should there be a quadratic reciprocity?

What about quadratic reciprocity over extensions of \( \mathbb{Q} \), like \( \mathbb{Q}(i) \), too!?!?

A preview... and example of the way that more classical \textit{reciprocity laws} are corollaries of fancier-looking things...: