In his 1921 thesis, E. Artin considered *hyperelliptic curves* over a finite field (of *odd* characteristic, for simplicity):

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

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 $\mathfrak{O} = \mathbb{F}_q[x, y]$, letting α be the image of x in $\mathbb{F}_q[x]/P \approx \mathbb{F}_{q^d}$,

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

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:

$$\begin{cases} \mathfrak{O}/\langle P\rangle \approx \mathbb{F}_{q^d} \oplus \mathbb{F}_{q^d} & \text{and } P\mathfrak{O} \approx \mathfrak{P}_1 \cap \mathfrak{P}_2 \qquad (\text{if } f(\alpha) \in (\mathbb{F}_{q^d})^{\times 2}) \\ \\ \mathfrak{O}/\langle P\rangle \approx \mathbb{F}_{q^{2d}} & \text{and } P\mathfrak{O} = \text{prime in } \mathfrak{O} \quad (\text{if } f(\alpha) \notin (\mathbb{F}_{q^d})^{\times 2}) \end{cases}$$

Example: for $y^2 = x^2 + 1$ over $\mathbb{F}_3$,

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

$$\mathfrak{O}/\langle x+1\rangle \;\approx\; \mathbb{F}_3[x,t]/\langle x+1, t^2 - x^2 - 1\rangle \;\approx\; \mathbb{F}_3[t]/\langle t^2 - 2\,\rangle \;\approx\; \mathbb{F}_{3^2}$$

$$\mathfrak{O}/\langle x-1\rangle \;\approx\; \mathbb{F}_3[x,t]/\langle x-1, t^2 - x^2 - 1\rangle \;\approx\; \mathbb{F}_3[t]/\langle t^2 - 2\,\rangle \;\approx\; \mathbb{F}_{3^2}$$

$$\mathfrak{O}/\langle x^2+1\rangle \approx \mathbb{F}_3[x,t]/\langle x^2+1, t^2-x^2-1\rangle \approx \mathbb{F}_{3^2}[t]/\langle t^2\,\rangle \approx \text{not product}$$

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

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

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

Is α^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?

$$\mathfrak{O}/\langle x^3 - x + 1\rangle \approx \mathbb{F}_3[x,t]/\langle x^3 - x + 1, t^2 - x^2 - 1\rangle$$
$$\approx\ \mathbb{F}_3(\alpha)[t]/\langle t^2 - \alpha^2 - 1\rangle \qquad\qquad (\text{with } \alpha^3 - \alpha + 1 = 0)$$

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:

$$f(\alpha) \in \mathbb{F}_p(\alpha)^{\times 2} \quad \Longleftrightarrow \quad f(\alpha)^{\frac{q^{d-1}}{2}} = 1$$

What should *quadratic reciprocity* be here? *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 *reciprocity laws* are corollaries of fancier-looking things... :

Let k be a *global field*, that is, either a *number field* (=finite extension of $\mathbb{Q}$) or *function field* (=finite separable extension of $\mathbb{F}_q(X)$), with integers $\mathfrak{o}$.

Let v index the *completions* k_v of k.

Let K be a *quadratic* extension of k, and put

$$K_v \;=\; K \otimes_k k_v$$

K_v is two copies of k_v when the prime indexed by v *splits* or *ramifies*, and is a quadratic field extension of k_v otherwise:

$$K \otimes_k k_v \;\approx\; k[x]/\langle f\rangle \;\otimes_k\; k_v \;\approx\; k_v[x]/\langle f\rangle$$

$$\approx \begin{cases} k_v \times k_v \quad \text{(when } f \text{ has a zero in } k_v) \\ \\ \text{a quadratic extension (when } f \text{ has no zero in } k_v) \end{cases}$$

The Galois norm $N : K \to k$ certainly gives $N : K^\times \to k^\times$, and by *extension of scalars* $N : K_v^\times \to k_v^\times$.

Define the **local norm residue symbol** $\nu_v : k_v^\times \to \{\pm 1\}$ by

$$\nu_v(\alpha) \;=\; \begin{cases} +1 & (\text{for } \alpha \in N(K_v^\times)) \\ \\ -1 & (\text{for } \alpha \notin N(K_v^\times)) \end{cases}$$

Example: of the three quadratic extensions of $\mathbb{Q}_p$ with p odd, the extension $\mathbb{Q}_p(\sqrt{\eta})$, obtained by adjoining a square root of a non-square *local unit* $\eta \in \mathbb{Z}_p^\times$, has the property that *norm is a surjection on local units:*

$$N(\mathbb{Z}_p[\sqrt{\eta}]^\times) \;=\; \mathbb{Z}_p^\times$$

Proof: Let D be an integer so that D is a non-square mod p, and $E = \mathbb{Q}_p(\sqrt{D})$. First, show that norm is a surjection $\mathbb{F}_{p^2}^\times \to \mathbb{F}_p^\times$. Indeed,

$$N(x) \;=\; x \cdot x^p \;=\; x^{1+p} \qquad\qquad (\text{for } \mathbb{F}_{p^2}^\times \to \mathbb{F}_p^\times)$$

The multiplicative group $\mathbb{F}_{p^2}^\times$ is cyclic of order $p^2 - 1$, so taking $(p+1)^{th}$ powers surjects to the *unique* cyclic subgroup of order $p-1$, which must be $\mathbb{F}_p^\times$.

Given $\alpha \in \mathbb{Z}_p^\times$, take $a \in \mathbb{Z}$ such that $a = \alpha \bmod p\mathbb{Z}_p$, so $a^{-1}\alpha = 1 \bmod p\mathbb{Z}_p$. Norms are surjective mod p, so there is $\beta \in \mathbb{Z}_p[\sqrt{D}]$ such that $N\beta = a + p\mathbb{Z}_p$, and $N\beta^{-1} \cdot \alpha \in 1 + p\mathbb{Z}_p$.

The p-adic exp and log show that for odd p the subgroup $1 + p\mathbb{Z}_p$ of $\mathbb{Z}_p^\times$ consists entirely of *squares*. Thus, there is $\gamma \in \mathbb{Z}_p^\times$ such that $\gamma^2 = N\beta^{-1} \cdot \alpha$, and then $\alpha = N(\beta\gamma)$. ///

A small *local* Theorem:

$$[k_v^\times : N(K_v^\times)] \;=\; \begin{cases} 2 & \text{(when } K_v \text{ is a field)} \\ \\ 1 & \text{(when } K_v \approx k_v \times k_v) \end{cases}$$

About the proof: when K_v is $k_v \times k_v$, the extended local norm is just *multiplication* of the two components, so is certainly surjective. The interesting case is when K_v is a (separable) quadratic extension of k_v.

We call the assertion *local* because it only refers to *completions*, which, in fact, is much easier.

Let's postpone proof of this auxiliary result, but note a corollary, similar to *Euler's criterion* for things being squares:

Cor: ν_v is a group homomorphism $k_v^\times \to \{\pm 1\}$. ///

An immediate, if opaque, definition of *ideles*:

$$\mathbb{J} \;=\; \mathbb{J}_k \;=\; (\text{ideles of } k)$$

$$= \{\{\alpha_v\} \in \prod_v k_v^\times \;:\; \alpha_v \in \mathfrak{o}_v^\times \text{ for all but finitely-many } v\}$$

Let

$$\nu = \prod_v \nu_v \;:\; \mathbb{J} \;\longrightarrow\; \{\pm 1\}$$

A big *global* **Theorem:** ν is a $k^\times$-invariant function on $\mathbb{J}$. That is, it *factors through* $\mathbb{J}/k^\times$. Other nomenclature: ν is a *Hecke character*, and/or a *grossencharakter*.

Granting this perhaps-unexciting-sounding feature, we can make some interesting deductions: ...

Quadratic Hilbert symbols

For $a, b \in k_v$ the (quadratic) **Hilbert symbol** is

$$(a,b)_v \;=\; \begin{cases} 1 & (\text{if } ax^2 + by^2 = z^2 \text{ has non-trivial solution in } k_v) \\ \\ -1 & (\text{otherwise}) \end{cases}$$

Memorable theorem: For $a, b \in k^\times$

$$\Pi_v \; (a,b)_v \;=\; 1$$

Proof: We prove this from the fact that the quadratic norm residue symbol is a Hecke character.

When b (or a) is a square in $k^\times$, the equation

$$ax^2 + by^2 \;=\; z^2$$

has a solution over k. There is a solution over k_v for all v, so all the Hilbert symbols are 1, and reciprocity holds in this case.

For b *not* a square in $k^\times$, rewrite the equation

$$ax^2 \;=\; z^2 - by^2 \;=\; N(z + y\sqrt{b})$$

and $K = k(\sqrt{b})$ is a quadratic field extension of k.

At a prime v of k *split* (or ramified) in K, the local extension $K \otimes_k k_v$ is not a field, and the norm is a surjection, so $\nu_v \;\equiv\; 1$ in that case.

At a prime v of k *not* split in K, the local extension $K \otimes_k k_v$ *is* a field, so

$$ax^2 \;=\; z^2 - by^2$$

can have no (non-trivial) solution x, y, z even in k_v unless $x \neq 0$. In that case, divide by x and find that a is a norm if and only if this equation has a solution.

That is, $(a, b)_v$ is $\nu_v(a)$ for the field extension $k(\sqrt{b})$, and the reciprocity law for the norm residue symbol gives the result for the Hilbert symbol. ///

Now obtain the most traditional quadratic reciprocity law from the reciprocity law for the quadratic Hilbert symbol. Define the quadratic symbol

$$\left(\frac{x}{v}\right)_2 = \begin{cases} 1 & (\text{for } x \text{ a non-zero square mod } v) \\ 0 & (\text{for } x = 0 \text{ mod } v) \\ -1 & (\text{for } x \text{ a non-square mod } v) \end{cases}$$

Quadratic Reciprocity ('main part'): For π and ϖ two elements of $\mathfrak{o}$ generating distinct odd prime ideals,

$$\left(\frac{\varpi}{\pi}\right)_2 \left(\frac{\pi}{\varpi}\right)_2 = \Pi_v \, (\pi, \varpi)_v$$

where v runs over all *even or infinite* primes, and $(,)_v$ is the (quadratic) Hilbert symbol.

Proof (of main part) We claim that, since $\pi\mathfrak{o}$ and $\varpi\mathfrak{o}$ are odd primes,

$$(\pi, \varpi)_v \;=\; \begin{cases} \left(\frac{\varpi}{\pi}\right)_2 & \text{for } v = \pi\mathfrak{o} \\ \\ \left(\frac{\pi}{\varpi}\right)_2 & \text{for } v = \varpi\mathfrak{o} \\ \\ 1 & \text{for } v \text{ odd and } v \neq \pi\mathfrak{o}, \varpi\mathfrak{o} \end{cases}$$

Let $v = \pi\mathfrak{o}$. Suppose that there is a solution x, y, z in k_v to

$$\pi x^2 + \varpi y^2 \;=\; z^2$$

Via the ultrametric property, $\mathrm{ord}_v y$ and $\mathrm{ord}_v z$ are identical, and less than $\mathrm{ord}_v x$, since ϖ is a v-unit and $\mathrm{ord}_v \pi x^2$ is *odd*. Multiply through by π^{2n} so that $\pi^n y$ and $\pi^n z$ are v-units. Then that ϖ must be a square modulo v.

On the other hand, when ϖ is a square modulo v, use Hensel's lemma to infer that ϖ is a square in k_v. Then

$$\varpi y^2 \;=\; z^2$$

certainly has a non-trivial solution.

For v an odd prime distinct from $\pi\mathfrak{o}$ and $\varpi\mathfrak{o}$, π and ϖ are v-units. When ϖ is a square in k_v, $\varpi \;=\; z^2$ has a solution, so the Hilbert symbol is 1. For ϖ not a square in k_v, $k_v(\sqrt{\varpi})$ is an *unramified** field extension of k_v, since v is odd. Thus, the norm map is surjective to units in k_v. Thus, there are $y, z \in k_v$ so that

$$\pi \;=\; N(z + y\sqrt{\varpi}) \;=\; z^2 - \varpi y^2$$

Thus, all but even-prime and infinite-prime quadratic Hilbert symbols are quadratic symbols. ///

Simplest examples Let's recover quadratic reciprocity for two (positive) odd prime numbers p, q:

$$\left(\frac{q}{p}\right)_2 \left(\frac{p}{q}\right)_2 \;=\; (-1)^{(p-1)(q-1)/4}$$

We have

$$\left(\frac{q}{p}\right)_2 \left(\frac{p}{q}\right)_2 \;=\; (p,q)_2 (p,q)_\infty$$

Since both p, q are positive, the equation

$$px^2 + qy^2 \;=\; z^2$$

has non-trivial *real* solutions x, y, z. That is, the 'real' Hilbert symbol $(p,q)_\infty$ for the archimedean completion of $\mathbb{Q}$ has the value 1. Therefore, only the 2-adic Hilbert symbol contributes to the right-hand side of Gauss' formula:

$$\left(\frac{q}{p}\right)_2 \left(\frac{p}{q}\right)_2 \;=\; (p,q)_2$$

Hensel's lemma shows that the solvability of the equation above (for p, q both 2-adic units) depends only upon their residue classes mod 8. The usual formula is but one way of interpolating the 2-adic Hilbert symbol by elementary-looking formulas. ///

For contrast, let us derive the analogue for $\mathbb{F}_q[T]$ with q odd: for distinct *monic* irreducible polynomials π, ϖ in $\mathbb{F}_q[T]$,

$$\left(\frac{\varpi}{\pi}\right)_2 \left(\frac{\pi}{\varpi}\right)_2 \;=\; \left(\frac{-1}{\mathbb{F}_q}\right)_2^{(\deg \pi)(\deg \varpi)}$$

Proof: From the general assertion above,

$$\left(\frac{\varpi}{\pi}\right)_2 \left(\frac{\pi}{\varpi}\right)_2 \;=\; (\pi, \varpi)_\infty$$

where ∞ is the prime (valuation)

$$P \;\longrightarrow\; q^{\deg P}$$

This norm has local ring consisting of rational functions in t writable as power series in the local parameter $t_\infty = t^{-1}$. Then

$$\pi \;=\; t_\infty^{-\deg \pi}(1 + t_\infty(\ldots))$$

where $(1 + t_\infty(\ldots))$ is a power series in t_∞. A similar assertion holds for ϖ. Thus, if either degree is *even*, then one of π, ϖ is a local square, so the Hilbert symbol is $+1$.

When $t_\infty^{-\deg \pi}(1 \;+\; t_\infty(\ldots))$ is a non-square, $\deg \pi$ is odd. Nevertheless, *any* expression of the form

$$1 + t_\infty(\ldots)$$

is a local square (by Hensel). Thus, without loss of generality, we are contemplating the equation

$$t_\infty(x^2 + y^2) \;=\; z^2$$

The t_∞-order of the right-hand side is even.

If there is no $\sqrt{-1}$ in $\mathbb{F}_q$, then the left-hand side is t_∞-times a norm from the unramified extension

$$\mathbb{F}_q(\sqrt{-1})(T) \;=\; \mathbb{F}_q(T)(\sqrt{-1})$$

so has odd order. This is impossible. On the other hand if there is a $\sqrt{-1}$ in $\mathbb{F}_q$ then the equation has non-trivial solutions.

Thus, if neither π nor ϖ is a local square (i.e., both are of odd degree), then the Hilbert symbol is 1 if and only if there is a $\sqrt{-1}$ in $\mathbb{F}_q$. The formula given above is an elementary interpolation of this assertion (as for the case $k = \mathbb{Q}$). ///