Exploring the Galois group of the rational numbers
New breakthroughs

Jared Weinstein
Boston University
January 12, 2015
This talk discusses *reciprocity laws* in four phases of their development:

- **Classical**: Fermat, Euler, Gauss
- **Early 20th century**: Class field theory
- **Late 20th century**: Modular forms
- **21st century**: Arithmetic manifolds
Which integers $n$ are sums of two perfect squares?

Fermat showed it is enough to know which primes $p$ divide a sum of two squares (which are not divisible by $p$).
Given a prime $p$, when does $x^2 + y^2 \equiv 0 \pmod{p}$ have a solution with $xy \neq 0$?

Same as asking: when does $x^2 + 1 \equiv 0 \pmod{p}$ have a solution? When does $x^2 + 1$ factor modulo $p$?

Answer: Either when $p = 2$ or $p \equiv 1 \pmod{4}$. (Then $x = \left(\frac{p-1}{2}\right)!$ is a solution.)
What is a reciprocity law?

**Question**

Given an irreducible polynomial $f(x)$ with integer coefficients, is there a rule which, given a prime $p$, determines whether $f(x)$ is split modulo $p$?

*Split* means that $f(x)$ modulo $p$ is the product of distinct linear factors.

Such a rule will be called a *reciprocity law* for $f(x)$. 
For which primes $p$ is $f(x) = x^2 - 5$ split modulo $p$? Ignoring 2 and 5, these are the red primes in the table:

<table>
<thead>
<tr>
<th>$n$</th>
<th>Factorization of $f(n)$</th>
<th>$n$</th>
<th>Factorization of $f(n)$</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>$-2^2$</td>
<td>8</td>
<td>59</td>
</tr>
<tr>
<td>2</td>
<td>$-1$</td>
<td>9</td>
<td>$2^2 \cdot 19$</td>
</tr>
<tr>
<td>3</td>
<td>$2^2$</td>
<td>10</td>
<td>$5 \cdot 19$</td>
</tr>
<tr>
<td>4</td>
<td>11</td>
<td>11</td>
<td>$2^2 \cdot 29$</td>
</tr>
<tr>
<td>5</td>
<td>$2^2 \cdot 5$</td>
<td>12</td>
<td>139</td>
</tr>
<tr>
<td>6</td>
<td>31</td>
<td>13</td>
<td>$2^2 \cdot 41$</td>
</tr>
<tr>
<td>7</td>
<td>$2^2 \cdot 11$</td>
<td>14</td>
<td>191</td>
</tr>
</tbody>
</table>
Here are some reciprocity laws for \( f(x) \) of degree 2.

**Theorem**

\[ x^2 + x + 1 \text{ splits mod } p \iff p \equiv 1 \pmod{3}. \]

**Theorem**

\[ x^2 - 5 \text{ splits mod } p \iff p \equiv \pm 1 \pmod{5}. \]

**Theorem**

\[ x^2 - 2 \text{ splits mod } p \iff p \equiv \pm 1 \pmod{8}. \]

These laws all involve *congruence conditions* on \( p \).
Let $f(x) = x^2 + bx + c$, and let $D = b^2 - 4ac$.

**Theorem**

The splitting behavior of $f(x)$ modulo $p$ is determined by $p \pmod{D}$.

This is the quadratic reciprocity law, first proved by Gauss. Typically the theorem known as quadratic reciprocity refers to this formula:

$$\left( \frac{p}{q} \right) \left( \frac{q}{p} \right) = (-1)^{\frac{p-1}{2} \frac{q-1}{2}},$$

where $p$ and $q$ are distinct odd primes, and $\left( \frac{p}{q} \right)$ is 1 if $p$ is a square modulo $q$ and $-1$ otherwise.
What about polynomials of higher degree?

Example: \( f(x) = x^4 - 2 \). If \( f(x) \) splits modulo \( p \), then 2 has 4 distinct 4th roots modulo \( p \). In particular 2 is a square modulo \( p \) \( \implies p \equiv \pm 1 \pmod{8} \). But also one of the ratios between these roots has to be a solution to \( x^2 \equiv -1 \), so \( p \equiv 1 \pmod{4} \). Thus \( p \equiv 1 \pmod{8} \).

Here are the first few primes \( p \equiv 1 \pmod{8} \), with the primes for which \( f(x) \) splits shown in red.

17, 41, 73, 89, 97, 113, 137, 193, 233, 241, 257, 281, 313, 337, 353, 401, 409, 433, 449, 457, 521, 569, 577, 593, 601, 617, 641,...
Gauss’ theorem on the biquadratic character of 2

**Theorem**

\[ x^4 - 2 \text{ splits modulo } p \text{ if and only if } p = x^2 + 64y^2. \]

This isn’t a congruence condition at all – at least not on \( p \) itself.
Gauss’ theorem on the biquadratic character of 2

**Theorem**

\[ x^4 - 2 \text{ splits modulo } p \text{ if and only if } p = x^2 + 64y^2. \]

However, if one writes

\[ p = a^2 + b^2, \] so that

\[ p = (a + bi)(a - bi), \] then Gauss’ criterion is equivalent to the statement that \( b \equiv 0 \pmod{8}, \) which is a congruence condition – not on \( p, \) but on \( a + bi! \)
Reciprocity laws in terms of number fields

The previous frame suggests that the splitting behavior of an irreducible polynomial $f(x)$ is linked with the arithmetic of the number field $K = \mathbb{Q}[x]/f(x)$.

The ring $\mathcal{O}_K$ (integral closure of $\mathbb{Z}$ in $K$) is a Dedekind domain, meaning that there is unique factorization of ideals into primes. So if $p$ is a prime we can write

$$p\mathcal{O}_K = p_1^{e_1} \cdots p_r^{e_r}.$$ 

for distinct prime ideals $p_1, \ldots, p_r$.

For all but finitely many bad (ramified) primes, all of the $e_i$ are 1. We say $p$ is split in $K$ if it is unramified and $r = [K : \mathbb{Q}]$.  

Jared Weinstein  
Exploring the Galois group of the rational numbers
Fermat’s theorem says that $p$ splits in $\mathbb{Q}(i) \iff p \equiv 1 \pmod{4}$.

**Question**

Let $L/K$ be an extension of number fields. Is there a rule for determining when a prime ideal of $K$ is split in $L$?

Let us call such a rule a *reciprocity law* for $L/K$. 
Example: the splitting field of $x^4 - 2$

Let $K = \mathbb{Q}(i)$, and let $L = K(2^{1/4})$. The theorems of Fermat and Gauss can be summarized this way:

\[
\begin{array}{c}
L \\
\downarrow \\
\pi \text{ splits } \iff \pi \equiv 1, 3, 5, 7 \pmod{8} \\
\downarrow \\
K \\
\downarrow \\
p \text{ splits } \iff p \equiv 1 \pmod{4} \\
\downarrow \\
\mathbb{Q}
\end{array}
\]

But there is no direct congruence condition determining when $p$ splits all the way from $\mathbb{Q}$ to $L$. 
Let $K = \mathbb{Q}(i)$, and let $L = K(2^{1/4})$. The Galois groups relating these fields are as follows:

Here $D_8$ is the dihedral group of order 8 (the symmetries of a square). It is \textit{not abelian}.
Theorem (c. 1940)

If $L/K$ is an abelian extension of number fields, then the splitting behavior of primes in $L/K$ is determined by congruence conditions.

This is the work of many people, including Artin (pictured), Hasse, Furtwängler, and Takagi.
This means we can come up with a reciprocity law for $L/K$ whenever $\text{Gal}(L/K)$ is a solvable group, such as $D_8$.

But as Abel showed, not all field extensions are solvable! What could a reciprocity law look like when $\text{Gal}(L/K)$ is an unsolvable group such as $A_5$?
Let $L/K$ be a Galois extension of number fields. Let $p$ is a prime of $K$ which is unramified in $L$, and let $\wp$ be a prime of $L$ dividing $p$. There exists a unique element $\text{Frob}_{\wp/p} \in \text{Gal}(L/K)$ such that

$$\text{Frob}_{\wp/p}(x) \equiv x^{N_p} \pmod{\wp}.$$ 

If a different prime $\wp'$ is chosen, the resulting Frobenii $\text{Frob}_{\wp}$ and $\text{Frob}_{\wp'}$ are conjugate in $\text{Gal}(L/K)$.

Thus we can talk about $\text{Frob}_p$ as a well-defined conjugacy class in $\text{Gal}(L/K)$.

Important fact: $\text{Frob}_p = 1 \iff p$ splits in $L$. 

Jared Weinstein  
Exploring the Galois group of the rational numbers
It is very useful to talk about all the extensions of $\mathbb{Q}$ at once, as living in $\overline{\mathbb{Q}}$. The *absolute Galois group* of $\mathbb{Q}$ is:

$$\text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) = \lim_{\leftarrow K} \text{Gal}(K/\mathbb{Q}),$$

where $K/\mathbb{Q}$ runs over finite Galois extensions.

The group $\text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ is utterly central to number theory. It is quite complicated, so instead of studying it directly, we study its *representations*. 
Example: a dihedral Galois representation

We can visualize generators of $D_8$ through its irreducible two-dimensional representation:

\[ r \quad s \]

Let \( \rho: \text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \text{GL}_2(\mathbb{C}) \)

be the representation which factors through \( \text{Gal}(\mathbb{Q}(i, 2^{1/4})/\mathbb{Q}) \cong D_8 \). Then \( \rho \) is unramified outside 2, and so \( \rho(\text{Frob}_p) \) makes sense as a conjugacy class in \( \text{GL}_2(\mathbb{C}) \) for each \( p \neq 2 \). In this case one has a simple rule for determining \( \rho(\text{Frob}_p) \)...
Example: a dihedral Galois representation

We can visualize generators of $D_8$ through its irreducible two-dimensional representation:

\[
\rho(Frob_p) = \begin{cases} 
1, & p = x^2 + 64y^2, \\
r^2, & p = x^2 + 16y^2, \ y \ \text{odd}, \\
rs, & p \equiv 3 \pmod{8} \\
r, & p \equiv 5 \pmod{8} \\
s, & p \equiv 7 \pmod{8}
\end{cases}
\]
These are special functions $g(\tau)$ on the upper half-plane $\mathcal{H}$, which are symmetric under certain substitutions, e.g. $\tau \mapsto \tau + 1$ and $\tau \mapsto -1/\tau$. 
Modular forms satisfy $g(\tau + 1) = g(\tau)$, so they have a Fourier expansion:

$$g(\tau) = \sum_{n \geq 0} a_n(g)q^n, \quad q = e^{2\pi i \tau}$$

A simple example is the sum $\sum_{n \in \mathbb{Z}} q^{n^2}$ (a form of weight $1/2$).

A variation on this idea: let

$$\theta_\chi(\tau) = \sum_{a \geq 0, \ b > 0} \chi(a + bi)q^{a^2+b^2}$$

where $\chi: \mathbb{Z}[i]/\mathfrak{f}^\times \rightarrow \mathbb{C}^\times$ is a nontrivial group homomorphism satisfying $\chi(i) = 1$. This is a modular form has weight 1.
Let
\[ \theta_{\chi}(\tau) = \sum_{a \geq 0, b > 0} \chi(a + bi)q^{a^2 + b^2} \]
where \( \chi: (\mathbb{Z}[i]/f)^\times \to \mathbb{C}^\times \) is a nontrivial group homomorphism satisfying \( \chi(i) = 1 \). This form has weight 1. An example of this: Let \( f = (8) \). There is a unique \( \chi \) with \( \chi(1 + 2i) = i \), and then

\[ a_p(\theta_{\chi}) = \begin{cases} 
2, & p = a^2 + 64b^2, \\
-2, & p = a^2 + 16b^2, \quad b \text{ odd}, \\
0, & \text{otherwise}
\end{cases} \]

This is always the same as \( \text{tr} \rho(\text{Frob}_p) \), where \( \rho: \text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \text{GL}_2(\mathbb{C}) \) is the Galois representation we encountered earlier.
Deligne’s theorem

Theorem (Deligne, 1971)

Let \( g \) be a cuspidal modular form which is an eigenvector for all Hecke operators. Then there exists

\[
\rho : \text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \text{GL}_2(\overline{\mathbb{Q}_\ell})
\]

such that \( \text{tr} \, \rho(\text{Frob}_p) = a_p(g) \) for almost all \( p \).
An icosahedral modular form

This example is due to Joe Bühler. Let $K$ be the splitting field of

$$f(x) = x^5 + 10x^3 - 10x^2 + 35x - 18.$$ 

Then $\text{Gal}(K/Q) \cong A_5$, the icosahedral group.

There exists a weight 1 cusp form of level 800 and character $\chi$

$$g(\tau) = q - iq^3 - ijq^7 - q^9 + jq^{13} + (i - ij)q^{19} - jq^{21} + \ldots,$$

where $i = \sqrt{-1}$ and $j = (1 + \sqrt{5})/2$.

**Theorem**

*For all $p \neq 2, 5$:*

\[ p \text{ splits in } K \iff a_p(g)^2 = 4\chi(p). \]
Modular curves

Modular forms are holomorphic functions on $\mathcal{H}$ which transform a certain way under an arithmetic subgroup $\Gamma \subset \text{SL}_2(\mathbb{Z})$. They are linked with the quotient spaces $\mathcal{H}/\Gamma$, which are algebraic curves called *modular curves*.

**Figure:** A fundamental domain for $\Gamma = \text{SL}_2(\mathbb{Z})$
The cohomology of modular curves is related to modular forms.

**Example**

Let $Y = \mathcal{H}/\Gamma$ and let $X$ be its compactification. Recall the Hodge decomposition

$$H^1(X, \mathbb{C}) = H^0(X, \Omega^1_{X/\mathbb{C}}) \oplus \overline{H^0(X, \Omega^1_{X/\mathbb{C}})}$$

If $f(\tau)\, d\tau \in H^0(X, \Omega^1_{X/\mathbb{C}})$ is a differential form, then $f(\tau)$ is a cusp form of weight 2.

Deligne's theorem can be rephrased this way: there are Galois representations attached to classes in $H^1(X, \mathbb{C})$ which are eigenvectors for the Hecke operators $T_p$. 
The upper half-plane $\mathcal{H} = \text{SL}_2(\mathbb{R})/\text{SO}(2)$ is a symmetric space. Others include:

- $\text{SL}_n(\mathbb{R})/\text{SO}(n)$
- $\mathcal{H}_3 = \text{SL}_2(\mathbb{C})/\text{SU}(2) \cong \mathbb{C} \times \mathbb{R}_{>0}$, a 3D hyperbolic space

An arithmetic manifold is the quotient of a symmetric space by an arithmetic subgroup. For instance the quotient of $\mathcal{H}_3$ by $\text{SL}_2(\mathbb{Z}[i])$ is an arithmetic manifold known as a Bianchi manifold. They are usually not complex manifolds, let alone algebraic varieties.
Many interesting hyperbolic 3-manifolds are arithmetic. (Image by Jeff Weeks.)
Let $M$ be an arithmetic manifold. The cohomology $H^i(M, \mathbb{C})$ has a commuting family of Hecke operators acting on it, one set for each prime.

The following theorem applies to a large class of arithmetic manifolds $M$ (coming from GL$_n$ over a real or CM field).

**Theorem (Harris-Lan-Taylor-Thorne, Scholze, 2012)**

Let $g \in H^i(M, \mathbb{C})$ be a Hecke eigenclass. There exists a Galois representation $\rho : \text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \text{GL}_n(\overline{\mathbb{Q}}_\ell)$, such that for almost all $p$, the conjugacy class $\rho(\text{Frob}_p)$ can be read off from the $p$th Hecke operators acting on $g$.

This theorem is difficult because (outside of the classical modular forms case) $M$ is not a algebraic variety.
Typically $H^i(M, \mathbb{Z})$ has a lot of torsion, whose arithmetic significance was uncertain until:

**Theorem (Scholze)**

To an eigenclass $g \in H^i(M, \overline{\mathbb{F}_p})$ be a Hecke eigenclass. There exists a corresponding Galois representation

$$\rho: \text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \text{GL}_n(\mathbb{F}_p).$$

This allows one to give reciprocity laws for many more $f(x)$!
To come up with the required $\rho$, one has to relate $H^i(M, \mathbb{F}_p)$ to $H^i(\text{Sh}, \mathbb{F}_p)$, where $\text{Sh}$ is a Shimura variety. It had been known before how to do this (Clozel). Get an eigenclass $f_0 \in H^i(\text{Sh}, \mathbb{F}_p)$. Want to get a congruence $f \equiv f_0 \pmod{p}$, where $f$ is an automorphic form. Galois representations had already been known to exist for such $f$.

It was essential to work with an infinite-level Shimura variety $\text{Sh}_p^\infty$, which lies atop a tower of varieties:

$$\text{Sh} \leftarrow \text{Sh}_p \leftarrow \text{Sh}_p^2 \leftarrow \cdots \leftarrow \text{Sh}_p^\infty.$$  

$\text{Sh}_p^\infty$ isn’t a manifold at all, but a fractal-like entity known as a perfectoid space.
Scholze proved a comparison isomorphism between mod $p$ étale and coherent cohomology of perfectoid spaces, which ultimately provides the link between $f_0$ and $f$. 
More on perfectoid spaces

Perfectoid spaces were originally invented by Scholze to solve a completely different problem (Deligne's weight-monodromy conjecture).

This problem had been solved previously over a Laurent series field $\mathbb{F}_p((t))$, but it was unknown how to solve it over the $p$-adic numbers $\mathbb{Q}_p$.

<table>
<thead>
<tr>
<th>Arithmetic in $\mathbb{Q}_5$:</th>
<th>Arithmetic in $\mathbb{F}_5((t))$:</th>
</tr>
</thead>
<tbody>
<tr>
<td>$\cdots$ 210.14</td>
<td>$\cdots$ 210.14</td>
</tr>
<tr>
<td>$\cdots$ 143.01</td>
<td>$\cdots$ 143.01</td>
</tr>
<tr>
<td>$\cdots$ 403.20</td>
<td>$\cdots$ 303.10</td>
</tr>
</tbody>
</table>

Jared Weinstein
Exploring the Galois group of the rational numbers
A key insight (due to Fontaine and Wintenberger in the 1970s) is that \( \mathbb{Q}_p \) and \( \mathbb{F}_p((t)) \) begin to look similar when you adjoin lots of \( p \)th power roots of \( p \) (respectively, \( t \)).

**Theorem**

Let \( K = \mathbb{Q}_p(p^{1/p^\infty})^\wedge \) and let \( K^b = \mathbb{F}_p((t^{1/p^\infty})) \). Then \( \text{Gal}(\overline{K}/K) \) and \( \text{Gal}(\overline{K^b}/K^b) \) are isomorphic.

The relation between \( K \) and \( K^b \) is:

\[
K^b = \{(x_0, x_1, x_2, \ldots) \mid x_i \in K, \ x_i^p = x_{i-1}\}
\]

Scholze generalized the process \( K \mapsto K^b \) to a much more general class of rings. In this way he was able to turn a problem over \( \mathbb{Q}_p \) into a problem over \( \mathbb{F}_p((t)) \), where it was previously known.
Open questions

- **Maass forms.** Is there a reciprocity law for quintic $f(x)$ with all real roots?

- **Modularity of $p$-adic Galois representations.** Does every $p$-adic Galois representation $\rho: \text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \text{GL}_n(\overline{\mathbb{Q}}_p)$ arise from some eigenclass $g$? (Kisin proved the $n = 2$ case, which is closely related to the proof of Fermat’s Last Theorem.)

- **Serre’s conjecture.** Does every mod $p$ Galois representation $\rho: \text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \text{GL}_n(\overline{\mathbb{F}}_p)$ arise from some mod $p$ eigenclass $g$?

Slides available at math.bu.edu/people/jsweinst/CEB.