RECIPROCITY LAWS
AND DENSITY THEOREMS

Richard Taylor
General problem: count the number of solutions to a FIXED polynomial(s) modulo a VARIABLE PRIME number.

RECIPROCITY LAW: a law which gives a completely different way to find the number of solutions for any given prime $p$.

DENSITY THEOREM: a theorem which describes the statistical behaviour of the number of solutions as the prime $p$ varies.
GAUSS’ LAW OF QUADRATIC RECIPROCITY (1796):

For any whole number \( n \) and prime number \( p \) the number of solutions to

\[ X^2 \equiv n \mod p \]

is 0, 1 or 2. For fixed \( n \) it depends only on \( p \mod 4n \).
How many solutions does $x^2 + 7 \equiv 0$ have modulo 32452843?

$32452843 = 1159030 \times 28 + 3$

Thus it has the same number of solutions as does

$x^2 + 7 \equiv 0 \pmod{3}$,

i.e. none.
DISTRIBUTION QUESTIONS

For what fraction of prime numbers \( p \) does \( x^2 + n \equiv 0 \) modulo \( p \) have 2 solutions? And what fraction 0 solutions?

THEOREM (Dirichlet, 1837): If \( -n \) is not a perfect square then for half the primes \( x^2 + n \equiv 0 \) modulo \( p \) has two solutions and for half the primes it has no solutions.
More precisely de la Vallée-Poussin showed in 1896 that

\[
\frac{\# \{ p \leq t : X^2 + n \equiv 0 \mod p \text{ has no solutions} \}}{\# \{ p \leq t \}}
\]

and

\[
\frac{\# \{ p \leq t : X^2 + n \equiv 0 \mod p \text{ has two solutions} \}}{\# \{ p \leq t \}}
\]

(where \( p \) denotes a variable prime number) both tend to 1/2 as \( t \) tends to infinity.

Both Dirichlet and de la Vallée-Poussin used Gauss’ law of quadratic reciprocity in an essential way.
What about higher degree polynomials of one variable?

There is a reciprocity theorem conjectured by Langlands, but it still seems to be far from being proved. It is not known even for a general quintic equation.

However, rather surprisingly, Dirichlet’s density theorem was extended to ALL one variable polynomial equations by Frobenius in 1880.
Example:

\[ X^4 - 2 = 0. \]

Its GALOIS GROUP \( G \) consists of all permutations of the roots

\[ \{ 4\sqrt{2}, i\sqrt{2}, -4\sqrt{2}, -i\sqrt{2} \} \]

which preserve all algebraic relations between them. For instance

\[ 4\sqrt{2} + (-4\sqrt{2}) = 0 \]

and so the pair \( \{ 4\sqrt{2}, -4\sqrt{2} \} \) must be taken either to itself or to the pair \( \{ i\sqrt{2}, -i\sqrt{2} \} \).
\[(\sqrt{2}, i\sqrt{2}, -\sqrt{2}, -i\sqrt{2})\]

\[(\sqrt{2}, -\sqrt{2})(i\sqrt{2}, -i\sqrt{2})\]

\[(\sqrt{2}, -i\sqrt{2}, -\sqrt{2}, i\sqrt{2})\]

\[c = (i\sqrt{2}, -i\sqrt{2})\]

\[(\sqrt{2}, -i\sqrt{2})(-\sqrt{2}, i\sqrt{2})\]

\[(\sqrt{2}, -\sqrt{2})\]

\[(\sqrt{2}, i\sqrt{2})(-\sqrt{2}, -i\sqrt{2})\]
There are 8 such permutations:

1 fixes all four roots;

2 fix just two roots; and

5 fix no roots.

Frobenius and de la Vallée-Poussin showed that
\[
\frac{\# \{ p \leq t : X^4 - 2 \equiv 0 \pmod{p} \text{ has 0 solutions} \}}{\# \{ p \leq t \}} \rightarrow \frac{5}{8}
\]

\[
\frac{\# \{ p \leq t : X^4 - 2 \equiv 0 \pmod{p} \text{ has 1 solution} \}}{\# \{ p \leq t \}} \rightarrow 0
\]

\[
\frac{\# \{ p \leq t : X^4 - 2 \equiv 0 \pmod{p} \text{ has 2 solutions} \}}{\# \{ p \leq t \}} \rightarrow \frac{1}{4}
\]

\[
\frac{\# \{ p \leq t : X^4 - 2 \equiv 0 \pmod{p} \text{ has 3 solutions} \}}{\# \{ p \leq t \}} \rightarrow 0
\]

\[
\frac{\# \{ p \leq t : X^4 - 2 \equiv 0 \pmod{p} \text{ has 4 solutions} \}}{\# \{ p \leq t \}} \rightarrow \frac{1}{8}
\]

as \( t \) goes to infinity.
What about equations with more variables?

For example (elliptic curves):

\[ Y^2 = X^3 + cX + d \]

\((c, d \text{ being fixed integers. Smooth, i.e. } 4c^3 + 27d^2 \neq 0. \) )

\[ j_E = 6912c^3/(4c^3 + 27d^2) \text{ is the } j\text{-invariant of } E. \]

How does the number \( N_p \) of solutions modulo \( p \) vary with a prime number \( p \)?
\[ E_0 : Y^2 + Y = X^3 - X^2 \]

<table>
<thead>
<tr>
<th>( p )</th>
<th>2</th>
<th>3</th>
<th>5</th>
<th>7</th>
<th>11</th>
<th>13</th>
<th>17</th>
<th>19</th>
<th>...</th>
</tr>
</thead>
<tbody>
<tr>
<td>( p - N_p )</td>
<td>-2</td>
<td>-1</td>
<td>1</td>
<td>-2</td>
<td>1</td>
<td>4</td>
<td>-2</td>
<td>0</td>
<td>...</td>
</tr>
</tbody>
</table>
\[ Y^2 + Y = X^3 - X^2 \]

<table>
<thead>
<tr>
<th>( p )</th>
<th>2</th>
<th>3</th>
<th>5</th>
<th>7</th>
<th>11</th>
<th>13</th>
<th>17</th>
<th>19</th>
<th>...</th>
</tr>
</thead>
<tbody>
<tr>
<td>( p - N_p )</td>
<td>-2</td>
<td>-1</td>
<td>1</td>
<td>-2</td>
<td>1</td>
<td>4</td>
<td>-2</td>
<td>0</td>
<td>...</td>
</tr>
</tbody>
</table>

\[ q \prod_{n=1}^{\infty} (1 - q^n)^2(1 - q^{11n})^2 = \]

\[ q - 2q^2 - q^3 + 2q^4 + q^5 + 2q^6 - 2q^7 \]

\[ -2q^9 - 2q^{10} + q^{11} - 2q^{12} + 4q^{13} + 4q^{14} \]

\[ -q^{15} - 4q^{16} - 2q^{17} + 4q^{18} + 2q^{20} + ... \]
\[ Y^2 + Y = X^3 - X^2 \]

<table>
<thead>
<tr>
<th>( p )</th>
<th>2</th>
<th>3</th>
<th>5</th>
<th>7</th>
<th>11</th>
<th>13</th>
<th>17</th>
<th>19</th>
<th>…</th>
</tr>
</thead>
<tbody>
<tr>
<td>( p - N_p )</td>
<td>-2</td>
<td>-1</td>
<td>1</td>
<td>-2</td>
<td>1</td>
<td>4</td>
<td>-2</td>
<td>0</td>
<td>…</td>
</tr>
</tbody>
</table>

\[
q \prod_{n=1}^{\infty} (1 - q^n)^2 (1 - q^{11n})^2 = \\
q - 2q^2 - q^3 + 2q^4 + q^5 + 2q^6 - 2q^7 \\
-2q^9 - 2q^{10} + q^{11} - 2q^{12} + 4q^{13} + 4q^{14} \\
-q^{15} - 4q^{16} - 2q^{17} + 4q^{18} + 2q^{20} + …
\]

**THEOREM** (Eichler, 1954)

\( p - N_p \) is the coefficient of \( q^p \).
\[ f(z) = e^{2\pi iz} \prod_{n=1}^{\infty} (1 - e^{2n\pi iz})^2 (1 - e^{22n\pi iz})^2 = \sum_{n=1}^{\infty} a_n e^{2n\pi iz} \]

\[
\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z}) \text{ with } 11 | c \text{ implies }
\]

\[ f((az + b)/(cz + d)) = (cz + d)^2 f(z) \]

Also

\[ f(-1/(11z)) = -11z^2 f(z) \]
TANIYAMA(’55)-SHIMURA(’57)-WEIL(’67) CONJECTURE: Gives a somewhat similar effective algorithm for calculating $p - N_p$ for any elliptic curve

$$E : \quad Y^2 = X^3 + cX + d \quad \text{(smooth)}.$$ 

Proved (Breuil, Conrad, Diamond, T: 2001) following ideas introduced by Wiles.
The algorithm involves finite index subgroups of $GL_2(\mathbb{Z})$ the group of $2 \times 2$ matrices with whole number entries and determinant $\pm 1$ and its action on the hyperbolic plane.
LANGLANDS in the mid 1970’s proposed a similar reciprocity law for any system of polynomial equations in any number of variables in terms connected to subgroups of finite index in $GL_n(\mathbb{Z})$ for variable $n$. 
We are beginning to make progress. For example Tom Barnet-Lamb (2009) has proved a reciprocity for

\[ X_1^5 + X_2^5 + X_3^5 + X_4^5 + X_5^5 = aX_1X_2X_3X_4X_5 \]

for \( a \in \mathbb{Q} - \mathbb{Z}[1/10] \) in terms of \( GL_4(\mathbb{Z}) \) and \( GL_2(\mathbb{Z}) \). He deduces the meromorphic continuation and functional equation of the \( \zeta \)-function.
DENSITY THEOREMS IN > 1 VARIABLE

\[ E : Y^2 = X^3 + cX + d \]

THEOREM (Hasse, 1933): \(|p - N_p| < 2\sqrt{p}|.

QUESTION: How is the normalised error term \((p - N_p)/\sqrt{p}\) distributed as \(p\) varies?
CONJECTURE (Sato-Tate, 1963):
If \( E \) is not CM then \((p - N_p)/\sqrt{p}\) is distributed in the range from \(-2\) to \(2\) like

\[
(1/2\pi)\sqrt{4 - t^2} \; dt.
\]

i.e. for \( f \in C[-2, 2] \)

\[
\#\{p \leq x\}^{-1} \sum_{p \leq x} f((p - N_p)/\sqrt{p})
\]

tends to

\[
(1/2\pi) \int_{-2}^{2} f(t) \sqrt{4 - t^2} \; dt
\]

as \( x \to \infty \).
SATO-TATE DISTRIBUTION
FOR $\Delta$ AND $p < 1,000,000$

(drawn by WILLIAM STEIN)
THEOREM (CHSBT, 2006): True if $j_E \in Q - Z$.

There exist conjectural generalizations to any number of polynomial equations in any number of variables.
\[ SU(2) / \text{conjugacy} \sim \{ -2, 2 \} \]

\[ [g] \mapsto \text{tr } g \]

Haar measure \leftrightarrow (1/2\pi)\sqrt{4 - t^2} \, dt

\[ [F_p / \sqrt{p}] \mapsto (p - N_p) / \sqrt{p}, \]

where \([F_p] \subset GL_2(\overline{Q})\) has characteristic polynomial

\[ X^2 - (p - N_p)X + p. \]

(Frobenius conjugacy class.)
The Sato-Tate conjecture says that the conjugacy classes

$$[F_p/\sqrt{p}]$$

are equidistributed in $SU(2)/$conjugacy with respect to Haar measure.

We have to prove that for all $f \in C[-2,2]$

$$\left( \sum_{p \leq x} f(\text{tr } F_p/\sqrt{p}) \right) / \# \{ p \leq x \}$$

tends to

$$(1/2\pi) \int_{-2}^{2} f(t)\sqrt{4 - t^2} \, dt$$

as $x \to \infty$.  

25
The Peter-Weyl theorem tells us that the functions

\[ \text{tr Sym}^{n-1} \]

for \( n = 1, 2, 3, \ldots \) span a dense subspace of \( C[SU(2)/\text{conjugacy}] = C[-2, 2] \).

Hence it suffices to show that

\[
\left( \sum_{p \leq x} \text{tr Sym}^{n-1}(F_p/\sqrt{p}) \right) / \#\{p \leq x\}
\]

tends to \( 1 \) if \( n = 1 \) (clear) and tends to \( 0 \) if \( n > 1 \).
L-FUNCTIONS: We define a holomorphic function

\[ L(\text{Symm}^{n-1}E, s) \]

in \( \text{Re } s > (n + 1)/2 \) by

\[ \prod_p \det(1_n - (\text{Symm}^{n-1}F_p)/p^s)^{-1}. \]

e.g.

\[ L(\text{Symm}^0E, s) = \zeta(s) \]

\[ L(\text{Symm}^1E, s) = L(E, s) \]
Taking logarithmic differentials we see that

\[ L'(\text{Symm}^{n-1} E, s)/L(\text{Symm}^{n-1} E, s) \]

differs from

\[ - \sum_p (\log p) (\text{tr Symm}^{n-1}(F_p/\sqrt{p})) p^{(n-1)/2-s} \]

by a function holomorphic in \( \text{Re } s > n/2 \).

Tauberian theorems tell us it suffices that the ratio is holomorphic in \( \text{Re } s \geq (n + 1)/2 \).
i.e. that

\[ L(\text{Symm}^{n-1}E, s) \]

is holomorphic and non-zero in

\[ \text{Res} \geq \frac{n + 1}{2} \]

for \( n > 1 \).

Gelbart-Jacquet (1972): this is true IF Symm\( ^{n-1}E \) satisfies a reciprocity law involving \( GL_n(Z) \).