Boylan
6-14-12
pg 1

Polynomials equations modulo p:

1) Quadratic equation: $f(x) = x^2 - x - 1$.

$$n(p) = |\{x \pmod p : f(x) \equiv 0 \pmod p\}| = 1 + \left(\frac{5}{p}\right) = 1 + \left(\frac{p}{5}\right)$$

$$= \begin{cases} 0 & p \equiv 2,3\ (5) \\ 1 & p = 5 \\ 2 & p \equiv 1,4\ (5). \end{cases}$$

roots: $\frac{1 \pm \sqrt{5}}{2}$.

Fix $j \in \{0,2\}$. $\delta(\{p : n(p) = j\}) = 1/2$

$\uparrow$ density.

2) Cubic equations: $f(x) = x^3 - x - 1$.

$\mathrm{disc}(f) = -23$

Note: $f(x) \equiv (x-3)(x-10)^2 \pmod{23}$

$\Rightarrow n(23) = 2$.

$\forall p \neq 23$, $n(p) \in \{0,1,3\}$.

Questions: Fix $j \in \{0,1,3\}$.

1) Formula/generating function for $n(p)$? $(1 + a(p)?)$
   Answer arises from modular forms.
2) Describe $\{p : n(p) = j\}$.
3) Compute $\delta(\{p : n(p) = j\})$.

] algebraic number theory.

Def: $f_{23}(q) = q \prod_{m=1}^{\infty} (1-q^m)(1-q^{23m})$, $|q| < 1$.

$\{a(n)\}$ $\quad f_{23}(q) = \sum_{n=1}^{\infty} a(n) q^n = q - q^2 - q^3 + q^6 + \cdots$

Theorem: $\forall p$, $n(p) = 1 + a(p)$.

Modular forms:

$$\mathfrak{h} = \{ z \in \mathbb{C} : \operatorname{Im}(z) > 0 \}$$
$$\Gamma_0(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z}) : N \mid c \right\}.$$

$f : \mathfrak{h} \to \mathbb{C}$ is a modular form of weight $k \in \mathbb{Z}$ on $\Gamma_0(N)$ with Nebentype χ (Dirichlet character mod N) if

1) $\forall \gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_0(N)$
$$f(\gamma z) = \chi(d)(cz+d)^k f(z).$$
2) f is holomorphic on $\mathfrak{h}$ and at cusps.

$$q = e^{2\pi i z} \qquad f(z) = \sum_{n=0}^{\infty} a_f(n) q^n \in M_k(\Gamma_0(N), \chi).$$

$M_k(\Gamma_0(N), \chi) \supseteq S_k(\Gamma_0(N), \chi)$ cusp forms.

Def: $\eta(z) = q^{1/24} \prod_{m=1}^{\infty} (1 - q^m)$;

$$f_{23}(z) = \eta(z)\eta(23z). = \sum_{n=1}^{\infty} a(n) q^n = q + \cdots$$

Fact: $f_{23}(z) \in \underbrace{S_1\left(\Gamma_0(23), \left(\tfrac{\cdot}{23}\right)\right)}_{\dim_{\mathbb{C}} = 1}$

$\Rightarrow$ f_{23} is an eigenvector for all Hecke operators

$\Rightarrow \forall\, m,n,\ \gcd(m,n)=1,\quad a(mn)=a(m)a(n).$

Algebraic Number Theory:

$f(x) = x^3 - x - 1 \qquad \text{Roots} = \{\alpha_1, \alpha_2, \alpha_3\},\ H = \text{splitting field}$

$$\begin{tikzcd}[arrows=dash]
 & H \arrow[dl] \arrow[d] \arrow[dr] \arrow[ddrr] & & \\
\mathbb{Q}(\alpha_1) \arrow[ddr] & \mathbb{Q}(\alpha_2) \arrow[dd] & \mathbb{Q}(\alpha_3) \arrow[ddl] & \\
 & & & K = \mathbb{Q}(\sqrt{\operatorname{disc}(f)} = \sqrt{-23}) \arrow[dll] \\
 & \mathbb{Q} & &
\end{tikzcd}$$

$\operatorname{Gal}(H/\mathbb{Q}) \simeq S_3.$

$K \longleftrightarrow \mathbb{Z}/3\mathbb{Z}$

Basic idea:

Thm: (efg): $F/\mathbb{Q}$, # field, $p \in \mathbb{P}_{\mathbb{Q}}$ = primes of $\mathbb{Q}$.

- $(p) = p\mathcal{O}_F = \underbrace{\wp_1^{e_1} \cdots \wp_g^{e_g}}_{\text{unique}}$
- $\forall i,\ |\mathcal{O}_F/\wp_i| = p^{f_i}$

$$\Rightarrow \sum_{i=1}^{g} e_i f_i = [F:\mathbb{Q}]$$

$F/\mathbb{Q}$ Galois $\Rightarrow \forall i,\ e_i = e,\ f_i = f$

- $(p) = (\wp_1 \cdots \wp_g)^e$
- $efg = [F:\mathbb{Q}]$

Thm (Kummer): θ : alg. number with minimal poly. $f_\theta(x)$

$F = \mathbb{Q}[\theta]$. Let $p \in \mathbb{P}_\mathbb{Q}$, $p \nmid [\mathcal{O}_F : \mathbb{Z}[\theta]]$.

$$f_\theta(x) = h_1(x)^{e_1} \cdots h_g(x)^{e_g} \pmod{p}$$

with h_i irred. in $\mathbb{F}_p[x]$. We have

1) $\wp_i = (p, h_i(\theta)) \trianglelefteq \mathcal{O}_F$ prime
2) $(p) = \wp_1^{e_1} \cdots \wp_g^{e_g}$.
3) $\deg h_i = f_i$.

Frobenius: associate to $p \in \mathbb{P}_\mathbb{Q}$:

$F/\mathbb{Q}$ Galois number field, $(p) = \wp_1 \cdots \wp_g$.

$$\mathrm{Gal}\left(\mathcal{O}_F/\wp_i \,/\, \mathbb{Z}/p\mathbb{Z}\right) = \langle \sigma_p : x \mapsto x^p \rangle$$
$$\cong \mathbb{Z}/f\mathbb{Z}$$
$$\cong \underbrace{D_{\wp_i}}_{\text{decomposition group}} \leq \mathrm{Gal}(F/\mathbb{Q})$$

Then $\mathrm{Frob}_{\wp_i}$ is the element of $D_{\wp_i}$ corresponding to σ_p.

- $\mathrm{Frob}_p = \{\mathrm{Frob}_{\wp_i}\}$ ← conjugacy class in $\mathrm{Gal}(F/\mathbb{Q})$.

- $\cancel{\#} f = \mathrm{ord}(\mathrm{Frob}_p)$ in $\mathrm{Gal}(F/\mathbb{Q})$

Thm (Chebotarev): Let $\sigma \in \mathrm{Gal}(F/\mathbb{Q})$, $Cl(\sigma)$ = conjugacy class of σ in $\mathrm{Gal}(F/\mathbb{Q})$. We have

$$\delta\left(\{p \in \mathbb{P}_\mathbb{Q} : \mathrm{Frob}_p = Cl(\sigma)\}\right) = \frac{|Cl(\sigma)|}{|\mathrm{Gal}(F/\mathbb{Q})|}.$$

$f(x) = x^3 - x - 1$ $\qquad$ $n(p) = \#$ sols (mod p)

$$\begin{tikzcd}
 & H \arrow[dl, dash] \arrow[d, dash] \arrow[dr, dash] \arrow[drr, dash] & & \\
L_1 \arrow[dr, dash] & L_2 \arrow[d, dash] & L_3 \arrow[dl, dash] & K \arrow[dll, dash] \\
 & \mathbb{Q} & &
\end{tikzcd}$$

$n(p)$	$\mathcal{O}_{L_i}$		$\mathcal{O}_K$	$\mathcal{O}_H$	o(Frob$_p$ in $G_{H/\mathbb{Q}}$)
0	(p)	$(f=3)$	$Q_1 Q_2$	$R_1 R_2$	3
1	$\mathfrak{p}_1 \mathfrak{p}_2$	$(f_1 = 1,\ f_2 = 2)$	(p)	$R_1 R_2 R_3$	2
3	$\mathfrak{p}_1 \mathfrak{p}_2 \mathfrak{p}_3$	$(f_i = 1)$	$Q_1 Q_2$	$R_1 R_2 \ldots R_6$	1

$\underbrace{\qquad\qquad\qquad\qquad\qquad\qquad}_{efg}$

δ	
$\frac{1}{3}$	(2 3-cycles)
$\frac{1}{2}$	(3 2-cycles)
$\frac{1}{6}$	(id)

Note: H = Hilbert class field of $K = \mathbb{Q}(\sqrt{-23})$

$$\Rightarrow n(p) = \begin{cases} 0 \iff (p) = Q_1 Q_2 & \text{w/ } Q_i \text{: non-principal} \\ 3 \iff (p) = Q_1 Q_2 & \text{w/ } Q_i \text{: principal.} \end{cases}$$

$S_3 \longleftrightarrow GL_2(\mathbb{C})$:

Boylan
6-14-12
pg 6

			order	trace
id	$\longmapsto$	$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$	1	2
(123)	$\longmapsto$	$\begin{pmatrix} 0 & 1 \\ -1 & -1 \end{pmatrix}$	3	-1
(132)	$\longmapsto$	$(*)$	3	-1
(23)	$\longmapsto$	$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$	2	0
(13)	$\longmapsto$	$*$	2	0
(12)	$\longmapsto$	$*$	2	0

$$\begin{tikzcd}
\mathrm{Gal}(H/\mathbb{Q}) \arrow[d, "\cong"'] \arrow[dr, "\rho"] \arrow[drr, "\mathrm{Tr}\circ\rho"] & & \\
S_3 \arrow[r] & GL_2(\mathbb{C}) \arrow[r, "\mathrm{Tr}"'] & \mathbb{C}
\end{tikzcd}$$

Set $b(p) = \mathrm{Tr}(\rho(\mathrm{Frob}_p))$.

$n(p)$	$f = o(\mathrm{Frob}_p)$	$b(p)$
0	3	-1
1	2	0
3	1	2

$n(p) = 1 + b(p)$

Recall: $f_{23}(z) = \sum a(n) q^n = \eta(z)\eta(23z) \in S_1(\Gamma_0(23), (\frac{\cdot}{23}))$.

Thm: $n(p) = 1 + a(p)$.

<u>Thm (Deligne-Serre 1972):</u> Let $f = \sum a_f(n) q^n \in S_1(\Gamma_0(N), \chi)$.
be an eigenform for all Hecke operators. Then there exists a continuous, odd, irreducible representation

$$\rho_f : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to GL_2(\mathbb{C})$$

s.t. $\forall\, p \nmid N$,

$$Tr(\rho_f(\mathrm{Frob}_p)) = a_f(p)$$
$$\det(\rho_f(\mathrm{Frob}_p)) = \chi(p)$$

$$\begin{tikzcd}
G_{\mathbb{Q}} \arrow[d] \arrow[drr, "\rho_{23}"] & & & \\
G_{\mathbb{Q}}/\ker\rho_{23} \arrow[r, phantom, "\cong"] \arrow[d, leftrightarrow] & \mathrm{im}(\rho_{23}) \arrow[r, hook] & GL_2(\mathbb{C}) \arrow[r, "Tr"] & \mathbb{C} \\
G_{\overline{\mathbb{Q}}/F} & F = \#\text{ field} & &
\end{tikzcd}$$

Can then show $F = H$.