PART I

A. Prime numbers.

$$\textcircled{2}.\ 3.\ \underset{2^2+1^2}{\textcircled{5}}.\ 7.\ 11.\ \underset{3^2+2^2}{\textcircled{13}}.\ \overset{4^2+1^2}{\textcircled{17}}.\ 19.\ 23.\ \underset{5^2+2^2}{\textcircled{29}}.\ 31.\ \overset{6^2+1^2}{\textcircled{37}}.\ \underset{5^2+4^2}{\textcircled{41}}.\ 43.\ 47.\ \overset{7^2+2^2}{\textcircled{53}}\ \cdots$$

Q. Which of them are sum of two squares?

A. $p = x^2+y^2 \ (\exists x.y \in \mathbb{Z}) \iff p=2$ or $p = \begin{cases} 4n+1. \\ \cancel{4n-1} \end{cases}$

pf (NOTE THE ASYMMETRY)

$\Rightarrow$: $p \neq 2$: odd. $\begin{cases} x: \text{odd} \Rightarrow x^2: \text{odd},\ 4m^2+4m+1 \\ x: \text{even} \Rightarrow x^2: \text{even}\ \ 4m^2. \end{cases}$

$(x.y)$ must be (odd. even). $\Rightarrow x^2+y^2$ must be $4k+1$.

Groups. Rings. Fields

DID NOT USE p: PRIME

$\boxed{21 \equiv 1 \bmod 4 \text{ but not } x^2+y^2}$

ABOVE DON'T HOLD FOR ODD INTEGERS

$\Leftarrow$: ~~HARD~~

Lemma. $\boxed{p \text{ divides } x^2+1}$ $(\exists x \in \mathbb{Z}) \iff p=2$ or $p = 4n+1$

$\because$) $(\mathbb{Z}/p)^\times$ = cyclic gp of order $p-1$. $\{0.1.2.\cdots.p-1\}$

$x^2+1 \equiv 0 \bmod p \ \cdots \ x^2 = -1$ in the field $\mathbb{F}_p = \mathbb{Z}/p$

x : order 4 in $\mathbb{F}_p^\times$. (4th root of unity)

$\therefore p = 4n+1$.

Now consider $p = x^2+y^2 = (x+iy)(x-iy)$ p: prime or $(x+iy)(x-iy)$

in the ring $\mathbb{Z}[i]$, which is shown to be a Unique Factorization Domain

but p divides $(x+i)(x-i)$ for some x $\Rightarrow$ p cannot be a prime by Lemma

$\Rightarrow$ p decomposes in $\mathbb{Z}[i]$

THE SET OF PRIMES MANIFESTS THE ALGEBRAIC "ORDER" OF INTEGERS

$p = \alpha\beta\gamma\cdots$

$p^2 = |p|^2 = \underbrace{|\alpha|^2|\beta|^2|\gamma|^2}_{\text{all} \in \mathbb{Z}}\cdots$

$\therefore \begin{cases} p = \alpha \text{ or} \\ p = \alpha\bar{\alpha}. \end{cases}$

BEHAVIOUR OF PRIMES

Thm. $p \neq 2$: prime

$$\begin{cases} \cdot\ p = x^2+y^2 \iff p \equiv 1 \bmod 4 \\ \cdot\ p = x^2+2y^2 \iff p \equiv 1, 3 \bmod 8 \\ \cdot\ p = x^2-2y^2 \iff p \equiv 1, 7 \bmod 8. \end{cases}$$

[The ~~Basic~~ oldest example of Langlands corresp. for $GL(1)/\mathbb{Q}$]

(Quadratic Reciprocity).

Correspond to solving $\left.\begin{matrix} x^2+1=0 \\ x^2+2=0 \\ x^2-2=0 \end{matrix}\right\}$ in $\mathbb{F}_p$.

B. Equations to Fields.

- FLT. $x^n+y^n=z^n,\ n\geq 3\ (x,y,z\in\mathbb{Z}) \Rightarrow xyz=0$ $\Leftarrow$ Taniyama-Shimura Conj. [Special case of Langlands Correspondence for $GL(2)/\mathbb{Q}$].
- $x^4+y^4+z^4=w^4$

$ax^2+bx+c=0 \rightsquigarrow x=\dfrac{-b\pm\sqrt{b^2-4ac}}{2a}$

$\left(\begin{array}{l} ax^3+bx^2+cx+d=0 \rightsquigarrow \text{similar} \\ ax^4+bx^3+cx^2+dx+e=0 \rightsquigarrow \cdots \end{array}\right)$.

Thm. (Galois). No formula w/ radicals for eqn of deg ≥ 5.

$\longrightarrow$ Rethink the problem.

$ax^2+bx+c=0 \longrightarrow x\in K(\sqrt{b^2-4ac})$. $\forall K$: field.
$(a,b,c\in K)$

WANT TO DO THIS IN GENERAL ??

- Solving equations.

Ex. 1. $x^4+x^3+x^2+x+1=0$. $\quad y=x+\frac{1}{x}.\quad y^2=x^2+2+\frac{1}{x^2}$.

$x^2+x+1+\frac{1}{x}+\frac{1}{x^2}=0.\quad y^2+y-1=0.\quad y=\dfrac{-1\pm\sqrt{5}}{2}$.

$x^2-yx+1=0$. $\quad\left(x=\dfrac{y\pm\sqrt{y^2-4}}{2}=\dfrac{(-1\pm\sqrt{5})\pm\sqrt{10\mp2\sqrt{5}}}{4}\right)$

- Galois group. permutation of roots ($\boxed{\text{Symmetry}}$).

ζ: root $\Rightarrow \zeta^2, \zeta^3, \zeta^4$ are roots. $\zeta^5=1$.

$(x-\zeta)(x-\zeta^2)(x-\zeta^3)(x-\zeta^4)=0$.

$\{\zeta\mapsto\zeta,\ \zeta\mapsto\zeta^2,\ \zeta\mapsto\zeta^3,\ \zeta\mapsto\zeta^4\}\cong(\mathbb{Z}/5)^\times$

$$\begin{tikzcd} \mathbb{Q}(\zeta_5) \arrow[d, dash] \\ \mathbb{Q}(\sqrt{5}) \arrow[d, dash] \\ \mathbb{Q} \end{tikzcd}$$

Ex. 2. $x^4+1=0$ $\quad (x-\zeta)(x-\zeta^3)(x-\zeta^5)(x-\zeta^7)=0$.

$\zeta^8=1.\ \zeta^2,\zeta^4\neq 1$.

$$\begin{tikzcd} & \{1\} \arrow[dl, dash] \arrow[d, dash] \arrow[dr, dash] & \\ \{1,5\} \arrow[dr, dash] & \{1,7\} \arrow[d, dash] & \{1,3\} \arrow[dl, dash] \\ & (\mathbb{Z}/8)^\times & \end{tikzcd} \qquad \begin{tikzcd} & \mathbb{Q}(\zeta) \arrow[dl, dash] \arrow[d, dash] \arrow[dr, dash] & \\ \mathbb{Q}(\sqrt{-1}) \arrow[dr, dash] & \mathbb{Q}(\sqrt{2}) \arrow[d, dash] & \mathbb{Q}(\sqrt{-2}) \arrow[dl, dash] \\ & \mathbb{Q} & \end{tikzcd}$$

Ex. 3 $\rightarrow$ OVERLEAF

Thm (Kronecker-Weber).

Any eqn/$\mathbb{Q}$ w/ abelian (commutative) Gal. gp has roots in $\mathbb{Q}(\zeta_N)$. $\exists N\geq 1$
root of $\zeta^N=1$.

WANT TO KNOW GAL. GPS OF FIELD EXTENSIONS/$\mathbb{Q}$.

$\Updownarrow$

DECOMPOSITION LAW OF PRIMES (how the eqn's decompose/$\mathbb{F}_p$ for each p).

Algebra (over $\forall$field) $\rightsquigarrow$ Algebra (over $\mathbb{Q}$, ...) ... algebraic number theory

C. Fields to Galois Representations.

Thm (Irred. of cyclotomic polynomials)

$N \geq 1$. $\mathrm{Gal}(\mathbb{Q}(\zeta_N)/\mathbb{Q}) \xrightarrow{\sim} (\mathbb{Z}/N)^\times$

$(\zeta \mapsto \zeta^a) \longmapsto a \bmod N$

$$\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \twoheadrightarrow \mathrm{Gal}(\mathbb{Q}^{ab}/\mathbb{Q}) \xrightarrow{\sim} \hat{\mathbb{Z}}^\times := \varprojlim_N (\mathbb{Z}/N)^\times \cong \prod_{\ell:\text{prime}} \mathbb{Z}_\ell^\times.$$

$\overline{\mathbb{Q}}$: algebraic closure of $\mathbb{Q}$.

$\mathbb{Q}^{ab}$: maximal abelian extn of $\mathbb{Q}$.

NON-ABELIAN THEORY.

... WANT TO KNOW ALL REPRESENTATIONS of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$.

VECTOR SPACES ... LIN. ALG.

AMENABLE TO. FUNCTORIALITY [$\oplus$. $\otimes$. $*$, .. Sym. Λ. Ind. Res.]

PART II

REP. THEORY

2). GALOIS GP/$\mathbb{Q}$ ~~Decomp~~ KNOWS THE BEHAVIOR OF PRIMES.

(eqn's / $\mathbb{F}_p$. eqn's / $\mathbb{Q}_p$: p-adic fields ... $\mathbb{R} = \mathbb{Q}_p$ when $p = \infty$.)

rep R of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \longleftrightarrow$ rep R_p of $\mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p)$ for $\forall p$.

$R \longmapsto \{R_p\}_{p:\text{primes}}$

Global obj. $\rightsquigarrow$ Sequence of Local objects.

? criterion ... Langlands (modularity).

Local Langlands corresp.

$$\boxed{n\text{-dim'l rep'n } R_p \text{ of } \mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p) \longleftrightarrow \text{irred. rep. } \pi_p \text{ of } GL_n(\mathbb{Q}_p)}$$

$\{R_p\}_{p:\text{primes}}$ come from $R \iff \bigotimes_{p:\text{prime}} \pi_p$ [irred rep of $GL_n(\mathbb{A})$] factors thru $GL_n(\mathbb{Q})$ $\quad \mathbb{A} = \prod_{p:\text{prime}} \mathbb{Q}_p$.

MODULAR FORMS ($GL_2/\mathbb{Q}$) $\rightsquigarrow$ AUTOMORPHIC REPRESENTATION of GL_n. (or any Lie gp G).

ALG. GEOMETRY.

1). ABUNDANT SOURCE OF ~~ABUNDA~~ GAL REPS .... COHOMOLOGY OF ALGEBRAIC ~~GEOMETRY~~ VARIETIES / $\mathbb{Q}$.

X : variety / $\mathbb{Q}$ (MULTI-VAR. EQNS / $\mathbb{Q}$)

$\rightsquigarrow H^i(X \otimes \overline{\mathbb{Q}}, \overline{\mathbb{Q}}_\ell)$: ℓ-adic étale cohomology (Grothendieck)

$\circlearrowleft$ $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$.

... fin. dim. vector sp. / $\overline{\mathbb{Q}}_\ell$ ($\cong \mathbb{C}$ as fields).

PIC

ALG. NUMBER THEORY. Modularity (Taylor-Wiles) REP. THEORY.

GALOIS REPS. $\longleftrightarrow$ AUTOMORPHIC REPS.

$R : Gal(\overline{\mathbb{Q}}/\mathbb{Q}) \to GL_n(\overline{\mathbb{Q}}_\ell)$ $\qquad \pi \subset L^2(GL_n(\mathbb{Q}) \backslash GL_n(\mathbb{A}))$

$\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad \cong \otimes \pi_p$.

L-functions

Étale Cohomology (Grothendieck). $\qquad\qquad\qquad$ Symmetric Spaces (Shimura Variety)

MOTIVES (COHOMOLOGY OF ALG. VARS / $\mathbb{Q}$).

ALG. GEOMETRY.

REM

1) Corresp.... proven in very special cases.
[say self dual. regular. discrete series at one prime / CM-field]

2) Local corresp. is proven (Harris-Taylor) by global methods.

3). Geometric Analogue.

Spec $\mathbb{Z}$.	$\mathbb{Q}$.	Number fields	$Gal(\overline{\mathbb{Q}}/\mathbb{Q})$	Gal Reps
$\updownarrow$	$\updownarrow$	$\updownarrow$	$\updownarrow$	$\updownarrow$
Spec $\mathbb{C}[T]$.	$\mathbb{C}(T)$.	Function fields of Riemann Surface C	$\pi_1(C)$	local system (vect. bdl w/ flat conn.)

- Motives $\longrightarrow$ Gal reps.

family of varieties $/C$ $\longrightarrow$ local system $/C$. ${}^L G$-bdls. $\qquad$ Shimura Var: $Aut(V) \simeq G$

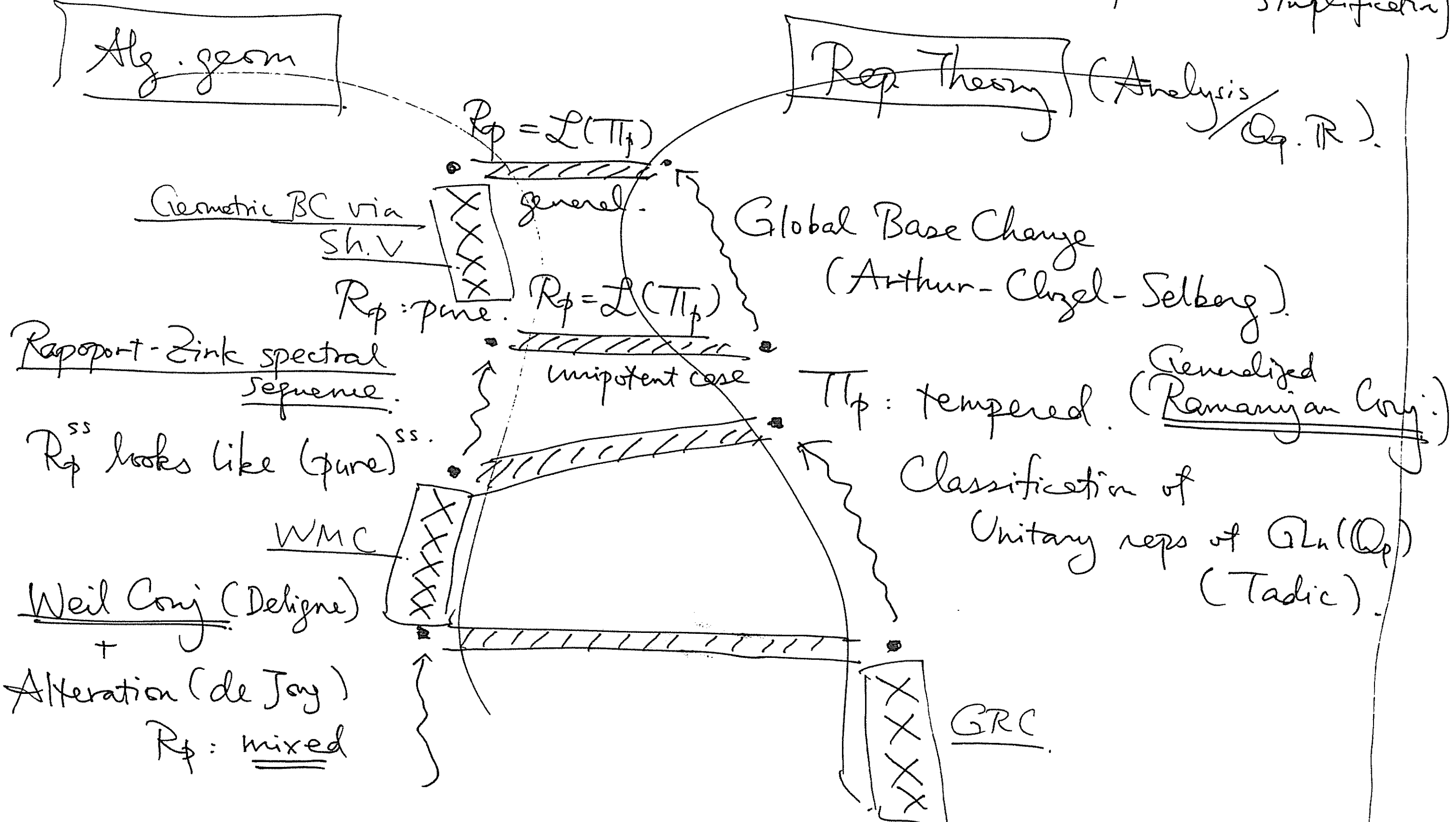
- Automorphic forms : ~~sections of vect. bdls~~ sheaves on moduli sp. of Hodge str. G.

$\rightsquigarrow$ Sheaves on moduli sp. of G-bdls $/C$.

LANDSCAPE WORK W/ TAYLOR.

IN THE CASES WHERE WE KNEW $R = \Pi$. Local L.C.

- WANTED TO SHOW $R_p \xleftrightarrow{\mathcal{L}} \Pi_p$ for all p.
- KNEW ~~$\mathcal{L}(R_p) = \Pi_p$~~ $R_p^{ss} = \mathcal{L}(\Pi_p)^{ss}$ (semi-simplification)



Ex. 3

$$X^4 + 52X^3 - 26X^2 - 12X + 1 = 0$$

(5-div. eqn of Lemniscatic curve $r^2 + r^4 = 2x^2$

$z(r) = \int_0^r \frac{dr}{\sqrt{1-r^4}}$ arc length

ζ : root

$$\Rightarrow \left\{ \zeta,\ \frac{-4\zeta}{(1-\zeta)^2},\ \frac{1-\zeta}{1+3\zeta},\ \frac{(1-\zeta)(1+3\zeta)}{-4\zeta^2} \right\}.$$

(Gauss' diary. 21/03/1797)

generates $\mathbb{Q}(\zeta_{20}) / \mathbb{Q}(i)$