Kevin Buzzard

6-27-08

Ken Ribet and Fermat's Last Theorem:

$$\begin{array}{c} X \\ \downarrow \varphi \\ Y \end{array}$$

non constant morphism of compact R.S.

"generic" $y \in Y$, then $\varphi^{-1}(y) = d$ distinct points

But there will be a finite (typically non-empty) "bad" set S of points of Y s.t. $\varphi^{-1}(s)$, $s \in S$ will have size $< d$.

A better invariant than the size of S is considering $e(x)$, $x \in X$ the multiplicity of x in $\varphi^{-1}(\{\varphi(x)\})$. Then for $s \in S$, we can consider

$$c(s) = \sum_{\substack{x \in X \\ \varphi(x) = s}} (e(x) - 1)$$

Then $\sum_{s \in S} c(s) \cdot s$ is a divisor on Y that holds much more information on Y.

Number theoretic counterpart:

$\mathbb{Z}[\sqrt{7}]$ $\quad 29 = (6+\sqrt{7})(6-\sqrt{7})$ $\quad 7 = (\sqrt{7})^2$ $\quad 2 = (3+\sqrt{7})^2 \cdot u$ ← unit.

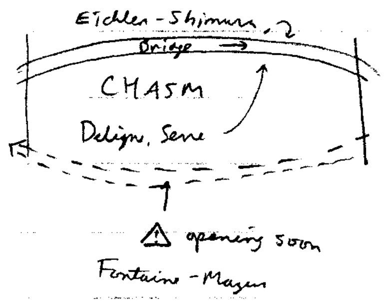
distinct primes

$\mathbb{Z}$ $\quad \ni 29$ $\quad 7$ $\quad 2$

Measure for the badness of primes in this situation would be the discriminant of $\mathbb{Z}[\sqrt{7}] = 28 = 2^2 \cdot 7$

In number theory sometimes an object has a "bad set" of primes and one can sometimes attach a positive integer $N = \prod_{p \in S} p^{c(p)}$ to the object, where $c(p)$ is an indicator of "how bad p is."

Modular forms
(analysis)



2-dim reps. of Galois groups
(arithmetic)

$f \rightsquigarrow \rho_f$ Eichler-Shimura: if $\ell \notin S(f)$, then

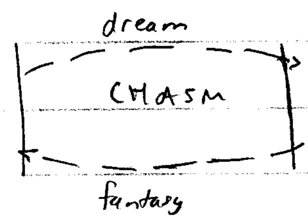
$S(f)$ $S(\rho_f)$ $\ell \notin S(\rho_f)$.

$N(f)$ $N(\rho_f)$

Thm (Deligne-Langlands-Carayol): In fact, $N(f) = N(\rho_f)$, i.e. "for a prime ℓ, f and ρ_f are exactly as bad as each other at ℓ."
"local-global compatibility" ($\ell \neq p$).

<u>More general picture:</u>

automorphic forms
(analysis)



n-dim. representations
of Galois groups

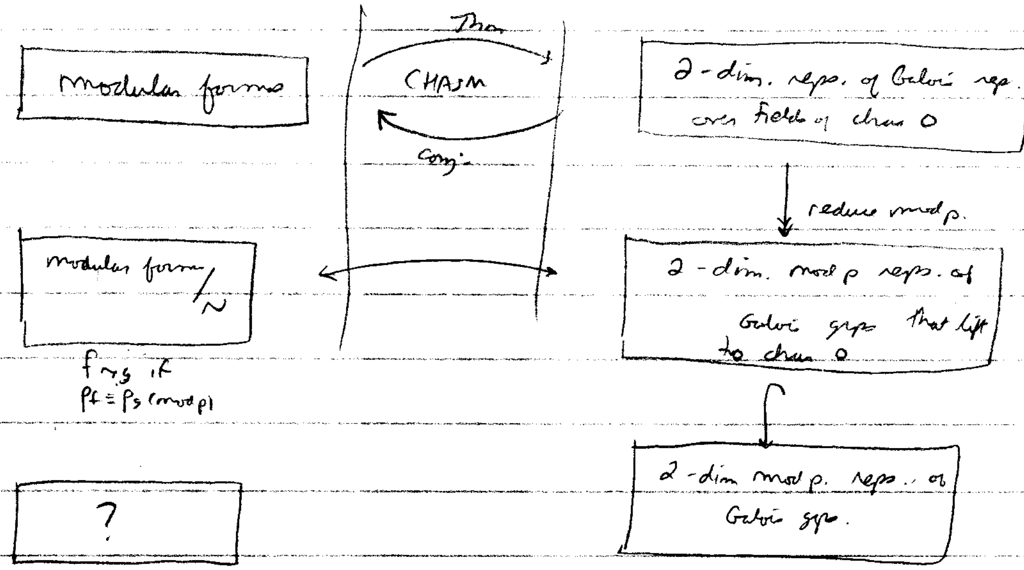
f, g ρ, σ

$f \oplus g \leftsquigarrow \rho \oplus \sigma$
very difficult!

$f \otimes g \leftsquigarrow \rho \otimes \sigma$
(only known in 2×2 and 2×3)

For certain unitary groups (Taylor-Yoshida 2007).

$f \rightsquigarrow \rho_f$ as bad as each other



$\text{level}([f]_\sim) := \min_{g \in [f]_\sim} N(g)$ $\underline{\underline{\quad\text{Ken}\quad}}$ $\text{cond}(\bar{\rho}) \in \mathbb{Z}_{\geq 1}$

What needs to be done? Start w/ f of level N. Get ρ_f of cond N, then get $\bar{\rho}_f$, cond $M \leq N$. Need to construct g s.t. $\bar{\rho}_f = \bar{\rho}_g$ and level of g is M.

<u>Application:</u> Say FLT is false, i.e. $\exists\ a, b, c \in \mathbb{Z}$, $p \geq 5$ prime s.t. $a^p + b^p = c^p$ and $abc \neq 0$.

Consider the elliptic curve

$$E : y^2 = x(x - a^p)(x + b^p).$$

Tate module of E is a char. 0 Galois rep. ρ

$$S(\rho) \text{ "=" } \{\ell : \ell \mid abc\}$$

But, $\text{cond}(\bar{\rho}) = 2$. Conjecture (Shim, Taniyama, Weil)

ρ on RHS of above. $\boxed{\text{If } \exists\ f \text{ on LHS s.t. } \rho = \rho_f}$, then Ken's Thm $\Rightarrow$ # as no appropriate g exists.