

Ramhw ABOELLATIF. - Du grand thèmerie de Fermat au programme de logarithms modulo p

RÉGA 14/12/11

p, l premiers distincts

I Motivations

1) Grand thm. de Fermat

Idee: si  $a^n + b^n = c^n$  avec  $abc \neq 0$ , alors on dispose de

$$E_{ab}: y^2 = x(x - a^n)(x + b^n)$$

Conj de Shimura - Taniyama - Weil

si  $E/\mathbb{Q}$  courbe elliptique de fonction  $L$  de Hasse - Weil  $L(E, s) = \sum_{n \geq 1} a_n n^{-s}$ ,

alors  $\sum a_n q^n$  est une forme modulaire de poids 2 et de niveau  $N_E$ .

Wils - Taylor: cas semi-stable

Breuil - Conrad - Diamond - Taylor (2003):

cas general

pour STW:  $\forall n, E[\ell^n] \cong (\mathbb{Z}/\ell^n \mathbb{Z})^2$

$$G_{\mathbb{Q}} = \text{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}) \cong E(\bar{\mathbb{Q}})$$

$$\leadsto E[\ell^\infty] = \mathbb{Z}_\ell \oplus \mathbb{Z}_\ell$$

on a donc:  $f: G_{\mathbb{Q}} \rightarrow GL_2(\mathbb{Z}_\ell)$   
 représentation  
 galoisienne  $\ell$ -adique

$$G_{\mathbb{Q}_p} = \text{Gal}(\bar{\mathbb{Q}}_p/\mathbb{Q}_p) \hookrightarrow G_{\mathbb{Q}} \xrightarrow{f} GL_2(\mathbb{Z}_\ell)$$

$\downarrow p$

Par ailleurs:

si  $f$  est une forme modulaire, on peut  
 lui associer  $\Pi_f = \Pi_{\infty} \otimes_p \Pi_p \cong GL_2(\mathbb{Q}_p)$   
 $\cup$   
 $GL_2(\mathbb{R})$

Fini de STW:  $f: G_{\mathbb{Q}} \rightarrow GL_2(\mathbb{Z}_\ell)$   
 $\downarrow$   
 $\bar{f} \rightarrow GL_2(\mathbb{F}_\ell)$

Idee: { définitions de  $\bar{f}$  }  $\rightarrow$  { def. de  $\bar{f}$  }  
 $G_{\mathbb{Q}} \rightarrow GL_2(\mathbb{Z}_\ell)$  } qui viennent  
 associées à des de  $F$  modulaires  
 caractères elliptiques

= si le 2<sup>ème</sup> ensemble  
 est non vide

