Last Theorem — Wiles' proof

Frey: ℓ premier impair, $a^\ell + b^\ell = c^\ell$ ~~solution non-triviale~~ $abc \neq 0$

a, b, c 2 à 2 premiers entre eux

on peut supposer : $a \equiv_2 1$, $b \equiv_2 0$

et plus $a^\ell \equiv_4 -1$ (si $a^\ell \equiv +1 \bmod 4$ multiplier par -1)

et $b^\ell \equiv_{32} 0$ (si $\ell \geq 5$)

Poser : $E : y^2 = \underbrace{x(x-a^\ell)(x+b^\ell)}_{\text{disc} = \pm (abc)^\ell}$

donc $E \bmod p$ singulier ssi $p \mid abc$

$\operatorname{cond}(E) = \prod_{p \mid abc} p$, donc E semi-stable

(réduction multiplic. pour les mauvais premiers)

$L = \mathbb{Q}(E[\ell])$

Fait : 1) L est ramifié seulement en 2 et ℓ, type de ramif. assez restreinte
(Description analytique de Tate de $E \bmod p$).

2) Soit $\rho : Gal(L/\mathbb{Q}) \hookrightarrow GL_2(\mathbb{F}_\ell)$ repr. associée
(ce qui identifie $E[\ell] \cong \mathbb{F}_\ell^2$)

$\ell \geq 13 \Rightarrow \rho$ surjective (on utilise ~~description de Mazur des types possibles pour $E(\mathbb{Q})_{tor}$~~ sous-groupe cyclique déf. sur $\mathbb{Q}$ i.e. $X_0(\ell)$ pt. rationnels cusp. Mazur)

Donc L très grand

Serre : conjecture : ρ irréductible et ρ impair (conjugaison complexe sur $E[\ell]$ est valeurs propres -1)

$\Rightarrow \rho \cong$ "$\rho_{f,\ell}$ modulo" où $f \in S_k(N)$, k, N convenables

on peut choisir $k = N = 2$

Mais : $S_2(2) = 0$