

$[F: \mathbb{Q}] < \infty$ ,  $F_\infty / F$  - a  $\mathbb{Z}_p$ -extension,  $\Gamma = \text{Gal}(F_\infty / F)$

$\Gamma \cong \mathbb{Z}_p$ ;  $\Gamma_n \subset \Gamma$ .  $[\Gamma: \Gamma_n] = p^n$ ,  $F_n = F_\infty^{\Gamma_n}$ ,  $\Gamma / \Gamma_n = \mathbb{Z}/p^n \mathbb{Z}$ .

$$F = F_0 \subset F_1 \dots \subset F_n \subset \dots \subset F_\infty$$

Every  $F$  has a unique  $\mathbb{Z}_p$ -extension  $F_\infty^{\text{cyc}} \subset F(\mu_{p^\infty})$ .

Iwasawa theory is a  $p$ -adic theory about arithmetic questions which uses  $\mathbb{Z}_p$ -extensions as the basic underlying tool.  $p$ -adic world.

### FACET 1. $F_\infty / F$

Iwasawa. Study behaviour of ideal class groups and units  $p$ -adically in the tower  $F_\infty / F$ , and their interpretation via global class field theory.

This is classical Iwasawa theory.

$S(s) = \prod_p (1 - p^{-s})^{-1}$  and its analytic continuation.

Important for arithmetic for two reasons: -

(a). Location of non-trivial zeroes  $\iff$  asymptotic distribution of prime numbers. (Riemann)

No known analogue in Iwasawa theory.

(b).  $S(1-n) \in \mathbb{Q}$  ( $n = 2, 4, 6, \dots$ )

Kummer: related to  $p$ -adic arithmetic of  $\mathbb{Q}(\mu_p)^+$ .

Leopoldt Kubota:  $p$ -adic analogue of  $S(s)$

Iwasawa made the great discovery that there appeared to be a precise relation between the zeroes of the Kubota-Leopoldt analogue of  $S(s)$  and the arithmetic of the tower  $\mathbb{Q}(\mu_{p^\infty})^+/\mathbb{Q}(\mu_p)^+$ .

Proved a beautiful general theorem in this direction in his great paper "On some modules in the theory of cyclotomic field".

Only proved his "main conjecture" when class number of  $\mathbb{Q}(\mu_p)^+$  is prime to  $p$ . Mazur & Wiles found the first proof that it holds for all  $p$ .

Arithmetic application to  $\mathbb{Z}$  itself: -

Quillen:  $K_{2n} \mathbb{Z} \cong \mathbb{Z} \quad (n=1, 2, \dots)$ .

Borel-Garland:  $K_{2n} \mathbb{Z}$  finite  $(n=1, 2, \dots)$ .

Birch-Tate, Lichtenbaum:

Theorem, For  $n=1, 2, \dots$

$$\#(K_{2n} \mathbb{Z}) = |w_n(\mathbb{Q}) S(\mathbb{Q}, 1-n)|.$$

Proof hinges on Iwasawa's "main conjecture".

Open problem. Prove the analogue for the Kubota-Leopoldt  $p$ -adic zeta function of the fact

Fact.  $S(s)$  has a simple zero at  $s = -2, -4, -6, \dots$

FACT 2.  $[F:\mathbb{Q}] < \infty$ ,  $M/F$  - a motive

Ex.  $F = \mathbb{Q}$ ,  $M =$  elliptic curve  $E/\mathbb{Q}$ .

Complex L-function.  $L(E, s)$  - entire by Deuring, Wiles, ...

Birch-Swinnerton-Dyer conjecture. Precise relation between  $E(\mathbb{Q})$  and  $\text{III}(E/\mathbb{Q})$  and behaviour of  $L(E, s)$  at  $s=1$ .

Only hope of proving exact formula for  $\#(\text{III}(E/\mathbb{Q}))$  in this conjecture is via Iwasawa theory.

Conjecture.  $L(E, 1) \neq 0 \Leftrightarrow E(\mathbb{Q})$  and  $\text{III}(E/\mathbb{Q})(p)$  finite for any prime  $p$ .

$\Rightarrow$  known for all  $p$  (Kolyvagin-Gross-Zagier).

$\Leftarrow$  known for  $p$  sufficiently large for "most"  $E$  by Iwasawa theory.

Key Remark. We need Iwasawa theory for every prime  $p$  to answer this type of question.

$E: y^2 = x^3 - N^2x$ , prove the above for  $p=2$ ?

Important because of Smith's recent work.

Goal. Prove the full BSD conjecture for every

$E/\mathbb{Q}$  such that  $L(E, s)$  has a zero at  $s=1$  of order  $\leq 1$ .

FACET 3. Carry out the analogue of Iwasawa theory when we replace the  $\mathbb{Z}_p$ -extension  $F_\infty/F$  by a Galois extension  $F_\infty/F$  whose Galois group is a compact  $p$ -adic Lie group e.g.  $GL_2(\mathbb{Z}_p)$ .

FACET 4. Most mysterious and very little is known about it at present.

General question. Prove that some of the classical Iwasawa modules are smaller than one would naively expect.

Iwasawa's  $\mu=0$  conjecture for  $F_\infty^{cyc}/F$ .  
Greenberg's conjectures.

End with an even more classical example, due to Weber ( $p=2$ ) and Fukuda-Komatsu in general.

Conjecture. Let  $p$  be any prime number,  $\mathbb{Q}_\infty/\mathbb{Q}$  the unique  $\mathbb{Z}_p$ -extension. Then the class number of every finite layer  $\mathbb{Q}_n$  of  $\mathbb{Q}_\infty/\mathbb{Q}$  is equal to 1.

Iwasawa proved class number of  $\mathbb{Q}_n$  is prime to  $p$ . How do we attack this even for  $p=2$ .

Overwhelming numerical evidence in support of conjecture.