1 Introduction

1.1 Arithmetic of $\mathbb{Q}(\zeta_p)$

We recall some basic facts about the arithmetic of the field $F := \mathbb{Q}(\zeta_p)$. For simplicity, write $\zeta$ instead of $\zeta_p$. Let $\mathcal{O}$ denote the ring of integers of $F$ and $\pi$ the element $1 - \zeta$. Certainly $\mathcal{O} \supseteq \mathbb{Z}[\zeta]$; we will see below that these rings are equal.

**Lemma 1.1.** $\mathcal{P} := (\pi)$ is a prime ideal in $\mathcal{O}$ and $\mathcal{P}^{p-1} = (p)$

*Proof.* Since 

$$1 + X + \cdots + X^{p-1} = \prod_{i=1}^{p-1} (X - \zeta^i)$$

we have

$$p = \prod_{i=1}^{p-1} (1 - \zeta^i) = (1 - \zeta)^{p-1} \cdot \prod_{i=1}^{p-1} \frac{1 - \zeta^i}{1 - \zeta}$$

But $(1 - \zeta^i) / (1 - \zeta)$ is a unit in $\mathcal{O}$ (why?), hence $\mathcal{P}^{p-1} = (p)$. By the degree formula, $\mathcal{P}$ must be a prime ideal. \qed

**Lemma 1.2.** $\mathcal{O} = \mathbb{Z}[\zeta]$

*Proof.* Let $\alpha \in \mathcal{O}$. Since $F = \mathbb{Q}(\pi)$ as well, we can write

$$\alpha = a_0 + a_1 \pi + \cdots + a_{p-2} \pi^{p-2}$$

with $a_i \in \mathbb{Q}$. By the previous lemma, $v_\pi(a_i)$ is a multiple of $p - 1$ for all $i$. Hence the valuations $v_\pi(a_i \pi^i)$ are all distinct. Thus $0 \leq v_\pi(\alpha) = \min_i v_\pi(a_i \pi^i)$ and this implies $v_\pi(a_i) \geq 0$ for all $i$. Thus all the $a_i$s are at least $p$-integers. Since $\pi = 1 - \zeta$,

$$\alpha = b_0 + b_1 \zeta + \cdots + b_{p-2} \zeta^{p-2}$$

for $b_i \in \mathbb{Q}$ being $p$-integers. Then

$$\text{Tr}(\alpha \zeta^{-j}) = pb_j - \sum_{i=0}^{p-2} b_i \in \mathbb{Z}$$

for all $j$, whence $p(b_j - b_0) \in \mathbb{Z}$ and so $b_j - b_0 \in \mathbb{Z}$ as well, since the $b_i$s are $p$-integers. Now

$$\alpha \equiv b_0(1 + \zeta + \cdots + \zeta^{p-2}) \mod \mathcal{O} \equiv -\zeta^{p-1} b_0 \mod \mathcal{O}$$

whence $b_0 \in \mathcal{O} \cap \mathbb{Q} = \mathbb{Z}$ as required. \qed

1.2 The first case of Fermat’s last theorem

We now show that the equation

$$x^p + y^p = z^p$$

has no solutions in positive integers $x, y, z$ with $p \nmid xyz$ and $p$ prime to the class group of $\mathbb{Q}(\zeta_p)$. For $p = 3$, we can check that this equation does not even admit solutions mod 9. So we assume
\( p \geq 5 \). We may also assume that \( x, y, z \) are pairwise coprime and that \( x \not\equiv y \mod p \) (why?). Now lets factorize the LHS in the equation above:

\[
(x + y)(x + \zeta y)(x + \zeta^2 y) \cdots (x + \zeta^{p-1} y) = z^p
\]

Lets’ note that the ideals \((x + \zeta^i y), (x + \zeta^j y)\) are coprime for \( i \neq j \) (why?). Hence, in particular,

\[
(x + \zeta y) = \mathfrak{a}^p
\]

for some ideal \( \mathfrak{a} \) in \( \mathcal{O} \). The above relation shows that \( \mathfrak{a}^p \) is a principal ideal. At this point we use the fact that the class number of \( F \) is prime to \( p \), which implies that \( \mathfrak{a} \) must be principal as well. So we can write

\[
x + \zeta y = \varepsilon \alpha^p
\]

for a unit \( \xi, \alpha \in \mathcal{O} \) with \( \varepsilon \) a unit. Next we use the following lemma about the structure of units in \( F \).

**Lemma 1.3.** Let \( \varepsilon \) be a unit in \( F \). Then \( \varepsilon = \zeta^r \varepsilon_1 \) for some integer \( r \) and some unit \( \varepsilon_1 \in F^+ \), where \( F^+ = \mathbb{Q}(\zeta + \zeta^{-1}) \) is the maximal totally real subfield of \( F \).

By the lemma

\[
x + \zeta y = \zeta^r \varepsilon_1 \alpha^p
\]

Now \( \alpha^p \equiv a \mod p \) for some rational integer \( a \) (why?). Hence

\[
x + \zeta y = \zeta^r \varepsilon_1 a \mod p
\]

and applying complex conjugation,

\[
x + \zeta^{-1} y = \zeta^{-r} \varepsilon_1 a \mod p
\]

as well. Thus

\[
x + \zeta y - \zeta^{2r} x - \zeta^{2r-1} y \equiv 0 \mod p
\]

If \( 1, \zeta, \zeta^{2r-1}, \zeta^{2r} \) are distinct, this would force \( x \) and \( y \) to be divisible by \( p \) (why?) which is a contradiction. If not, an easy case by case analysis (using that \( x \not\equiv y \mod p \) in the case \( 1 = \zeta^{2r-1} \)) can be used to achieve a similar contradiction. All we need now is a

**Proof.** (of Lemma above:) Let \( \xi = \varepsilon/\overline{\varepsilon} \). For all automorphisms \( \sigma \in \text{Gal}(F/\mathbb{Q}) \), \( |\xi^\sigma| = 1 \) since complex conjugation commutes with all such \( \sigma \). Thus \( \xi \) must be a root of unity (why?) in \( F \), hence \( \xi = \pm \zeta^t \) for some \( t \) (why?). Writing \( t = 2r, \varepsilon/\overline{\varepsilon} = \zeta^2r \), hence setting \( \varepsilon_1 = \varepsilon \zeta^{-r} \), we have \( \varepsilon_1/\overline{\varepsilon}_1 = \pm 1 \). Since \( \varepsilon_1 \equiv \overline{\varepsilon}_1 \mod \pi \) (why?), and \( p \neq 2 \), the sign must be +.

### 1.3 Goal of this class

As we have seen above, the question of whether or not \( p \) divides the class number of \( F = \mathbb{Q}(\zeta_p) \) turns out to have interesting applications to number theoretic problems. In 1847, Lamé presented a "proof" of Fermat’s last theorem to the French academy. Liouville, who was in attendance, promptly pointed out a gap, namely that Lamé had assumed the ring of integers of \( \mathbb{Z}[\zeta_p] \) was a UFD. In searching for a proof of this missing ingredient, they learned that three years earlier Kummer had already published a paper showing this to be untrue in general. The crucial question turns out to be, not whether \( \mathbb{Z}[\zeta_p] \) is a UFD but whether its class number can be divisible by \( p \).
Kummer called the primes $p$ for which this happens irregular primes. For primes that were regular (i.e. not irregular) he was able to demonstrate that Fermat’s last theorem was true for exponents divisible by such primes. As far as irregular primes go, he showed the following characterization.

**Theorem 1.4. (Kummer)** Let $B_n$ be the Bernoulli numbers defined by

$$\frac{t}{e^t - 1} = \sum_{n=0}^{\infty} B_n \frac{t^n}{n!}$$

Then $p$ is irregular iff $p$ divides the numerator of one of the numbers $B_2, B_4, \ldots, B_{p-3}$.

Note that the odd Bernoulli numbers are all zero except for $B_1 = -\frac{1}{2}$. The first few even Bernoulli numbers are $B_0 = 1, B_2 = \frac{1}{6}, B_4 = -\frac{1}{30}, B_6 = \frac{1}{42}, B_8 = -\frac{1}{30}, B_{10} = \frac{5}{66}, B_{12} = -\frac{691}{2730}, \ldots$. Thus 691 is an irregular prime. Surprisingly, it is not hard to show that there are infinitely many irregular primes; however we do not yet know if there are infinitely many regular primes!

What happened next?

- The Galois group $\text{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q})$ acts naturally on the $p$-part of the class group of $\mathbb{Q}(\zeta_p)$. Can one describe the sizes of the various eigencomponents for this action? How are these related to Bernoulli numbers?

  Stickelberger - Herbrand - Ribet: $p \mid B_m$ iff a particular piece of the $p$-part of the class group is nontrivial.

- Iwasawa’s idea: was that one should look not just at $\mathbb{Q}(\zeta_p)$ but the whole tower of fields $\mathbb{Q} \subset \mathbb{Q}(\zeta_p) \subset \mathbb{Q}(\zeta_{p^2}) \subset \cdots \subset \mathbb{Q}(\zeta_{p^n})$. Let $C_n$ denote the $p$-part of the ideal class group of $\mathbb{Q}(\zeta_{p^n})$. There are natural maps $C_1 \leftarrow C_2 \leftarrow \cdots$ (the norm maps), so we can take the inverse limit $C_\infty := \varprojlim C_n$ and consider it as a module for the action of $G_\infty := \text{Gal}(\mathbb{Q}(\zeta_{p^n})/\mathbb{Q}) \simeq \mathbb{Z}/(p-1)\mathbb{Z} \times \mathbb{Z}_p$. Iwasawa asked the following question.

**Question 1.5.** Can we describe the structure of $C_\infty$ as a $\mathbb{Z}_p[G_\infty]$ module?

Iwasawa conjectured (the main conjecture) that the structure of $C_\infty$ should be described by a certain ($p$-adic) analytic object called a $p$-adic $L$-function. Once consequence of this conjecture would be a very refined description of the various eigencomponents of $C_1$ for the action of $\text{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q})$.

The main conjecture was first proved by Mazur and Wiles (Inven. 1984) building on the techniques used by Ribet in his refinement of Kummer’s theorem mentioned above. This proof uses some rather sophisticated techniques from arithmetic geometry, namely the arithmetic of modular curves and a detailed study of the Galois representations associated to modular forms. Later on, another proof was found by Kolyvagin using ideas of Thaine. This proof proceeds via the construction of an “Euler system” is much more elementary.

- ’70s. Other kinds of $p$-adic $L$-functions were constructed eg. totally real fields (Deligne-Ribet), CM fields (Katz), ordinary elliptic curves (Mazur-Swinnerton-Dyer).

- Late ’80s - early ’90s: Main conjecture for imaginary quadratic fields: de Shalit, Tilouine, Rubin.
• More recently:
  Elliptic curves over $\mathbb{Q}$: Kato, Skinner-Urban.
  CM fields: Hida-Tilouine, Hida for the anticyclotomic $p$-adic $L$-function.

**Main goal of this class:** To formulate the main conjecture and present Rubin’s version of the proof of Thaine-Kolyvagin using Euler systems.

If this class were to continue next term, here are some natural possibilities:

• Modular forms and the Mazur-Wiles proof of the main conjecture.

• $p$-adic $L$-functions attached to imaginary quadratic fields and the relation with the arithmetic of CM elliptic curves.

**Exercises**

1. Let $\zeta_{p^n}$ denote a primitive $p^n$th root of unity. Show that the ring of integers of $\mathbb{Q}(\zeta_{p^n})$ is $\mathbb{Z}[\zeta_{p^n}]$.

2. Let $\alpha$ be an algebraic integer all whose conjugates have absolute value 1. Show that $\alpha$ must be a root of unity.