(VI.E) FERMAT’S LAST THEOREM FOR REGULAR EXPONENTS

We are now ready to exploit the unique factorization property of 𝔸(K), the monoid of (nonzero) integral ideals in 𝒪ₖ, to study the famous Diophantine equation

\[ x^m + y^m = z^m. \]

In order to disprove the existence of solutions with nonzero xyz, it is enough to show, for some prime \( p \mid m \), that \( x^p + y^p = z^p \) has no such solutions.

**Cyclotomic fields.** This suggests that it will be useful to consider the fields \( K = \mathbb{Q}(\zeta_p) \), where \( p \) is prime and \( \zeta_p = e^{\frac{2\pi i}{p}} \). The key results on these so-called cyclotomic fields, for our purposes, are the following:

**Fact 1.** \( K = \mathbb{Q}(\zeta_p) \implies \mathcal{O}_K = \mathbb{Z}[\zeta_p], [K : \mathbb{Q}] = p - 1. \)

While we won’t prove this, I should mention that the minimal polynomial of \( \zeta_p \) is not \( X^p - 1 \) but \( X^{p-1} = X^{p-1} + \cdots + X + 1 \) (which is irreducible over \( \mathbb{Q} \)); this explains the degree \( p - 1 \).

**Fact 2.** The embeddings \( \sigma_j : \mathbb{Q}(\zeta_p) \hookrightarrow \mathbb{C} \ (j = 1, \ldots, p - 1) \) are given by sending \( \zeta_p \mapsto \zeta_p^j \). Moreover they “respect” complex conjugation: \( \sigma_j(\bar{\alpha}) = \overline{\sigma_j(\alpha)} \).

This one is easy to see: we know there are \( [\mathbb{Q}(\zeta_p) : \mathbb{Q}] = p - 1 \) distinct embeddings; and the \( \{\sigma_j\} \) are clearly distinct as \( \zeta_p \) has distinct images under them. Moreover, an arbitrary element \( \alpha = \sum_{k=0}^{p-1} a_k \zeta_p^k \) \((a_k \in \mathbb{Q})\) has image \( \sigma_j(\alpha) = \sum a_k \sigma_j(\zeta_p)^k = \sum a_k \zeta_p^{jk} \), and so \( \sigma_j(\bar{\alpha}) = \sigma_j(\sum a_k \zeta_p^{-k}) = \sum a_k \bar{\zeta}_p^{-jk} = \sum a_k \bar{\zeta}_p^{jk} = \overline{\sigma_j(\alpha)} \). Next we have

\[^1\text{If } m > 2 \text{ is a power of } 2, \text{ then } 4 \mid m. \text{ We have already checked Fermat for the exponent } 4 \text{ in } \S IV.A.\]
Fact 3. The roots of unity in $K = \mathbb{Q}(\zeta_p)$ are just the $\pm \zeta_p^j$.

If you want to try to prove this, the hint is to first show that in general $[\mathbb{Q}(\zeta_m) : \mathbb{Q}] = \varphi(m)$ (clear for $m = p$ from the Fact 1), then ask what happens if $\mathbb{Q}(\zeta_m) = \mathbb{Q}(\zeta_p)$.

Fact 4 (Kummer's Lemma). If $u \in \mathbb{Z}[\zeta_p]^*$, then $u/\overline{u}$ is a root of unity (hence $\pm \zeta_p^j$).

This is an immediate consequence of the following more general

Lemma 5 (Kronecker). Let $K/\mathbb{Q}$ be an algebraic number field, and denote by $\sigma_1, \ldots, \sigma_n$ the $n$ embeddings $K \hookrightarrow \mathbb{C}$. If $\alpha \in \mathcal{O}_K$ is such that $|\sigma_j(\alpha)| \leq 1$ for all $j = 1, 2, \ldots, n$, then $\alpha$ is a root of unity.

Proof. Since $\alpha$ is an algebraic integer, it is a root of

$$f(x) = \prod_{j=1}^{n}(x - \sigma_j(\alpha)) = x^n + a_1x^{n-1} + \cdots + a_n$$

where $a_k \in \mathbb{Z}$ for each $k$. Since $|\sigma_j(\alpha)| \leq 1$ ($\forall j$), we have also $|a_k| \leq \left(\frac{n}{k}\right)$ for each $k$. There are only finitely many such polynomials. Moreover, if $\alpha$ satisfies the conditions of the Lemma, then so do its powers $\alpha^2, \alpha^3, \ldots$, which are therefore also among the finitely many roots of this set of polynomials. By the pigeonhole principle, two distinct powers of $\alpha$ must be equal. Thus, $\alpha$ is a root of 1. $\square$

Now Fact 4 follows as once, since (using Fact 2) $\sigma_j(u/\overline{u}) = \sigma_j(u)/\sigma_j(\overline{u}) = \sigma_j(u)/\overline{\sigma_j(u)}$ has absolute value 1 for each $j$.

Fermat’s equation. We are interested in the equation

$$(2) \quad x^p + y^p = z^p,$$

where $p > 3$ is prime. The proof that follows really won’t work for $p = 3$; fortunately, the exponent 3 can be dealt with by a direct “argument by descent” as carried out in §IV.A for exponent 4. We won’t bother with the details.
Suppose then that there exists a solution, with \( xyz \neq 0 \). If \( x, y, z \) have a common divisor, then of course we can strike it out to get a smaller solution. Assume this done. Now if any two of them still have a common factor \( m \), say \( m \mid x, y \), then \( m^p \mid z^p \implies (m, z) \neq 1 \), a contradiction. So we may assume \( x, y, z \) are pairwise relatively prime. Also, we will assume that \( p \) divides none of them. A separate, analogous (but more complicated) argument is needed to deal with the case where \( p \) divides exactly one of \( x, y, z \). We’ll omit this.

So assume \( p > 3 \) is prime, and \( (x, y, z) \) is a solution to (2) in pairwise coprime integers, none divisible by \( p \). We will now attempt to obtain a contradiction by passing to the cyclotomic number ring \( \mathbb{Z}[\zeta], \zeta = \zeta_p \), and factoring the left-hand side of (2) to obtain

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

**Case 1: \( \mathbb{Z}[\zeta] \) a UFD.** To get started, assume that \( h_{\mathbb{Q}(\zeta_p)} = 1 \), so that \( \mathbb{Z}[\zeta_p] \) is a unique factorization domain: i.e., every element has a factorization into prime elements which is unique up to reordering and units. As

\[
(t - \zeta)(t - \zeta^2) \cdots (t - \zeta^{p-1}) = \frac{t^p - 1}{t - 1} = 1 + t + \cdots + t^{p-1}
\]

evaluates to \( p \) at \( t = 1 \), we have the inclusion of principal ideals

\[
(p) \subset ((1 - \zeta^a))
\]

for each \( a = 1, 2, \ldots, p - 1 \). (Equivalently, \( (1 - \zeta^a) \mid p \).) The irreducibility of \( 1 + t + \cdots + t^{p-1} \) over \( \mathbb{Q} \) (implicit in Fact 1) implies that any element of \( \mathbb{Q}[\zeta] \) has a unique representation as \( a_0 + a_1\zeta + \cdots + a_{p-2}\zeta^{p-2} \).

Next let \( \pi \in \mathbb{Z}[\zeta] \) be a prime factor of \( x + y\zeta \). By unique factorization and (3), \( \pi \mid z \). If \( \pi \) also divides \( x + y\zeta^{a+1} \) (for some \( a = 1, \ldots, p - 1 \)), then it divides the \( \mathbb{Z}[\zeta] \)-linear combination \( \zeta^{-1}(x + y\zeta) - \zeta^{-1}(x + y\zeta^{a+1}) = y(1 - \zeta^a) \) hence \( yp \). Now in \( \mathbb{Z} \), \( \gcd(z, yp) \mid \gcd(z, y) \cdot \gcd(z, p) = 1 \cdot 1 = 1 \implies zm + ypm = 1 \) for some \( n, m \in \mathbb{Z} \). Since \( \pi \) divides \( z \) and \( yp \), we have \( \pi \mid 1 \implies \pi \in \mathbb{Z}[\zeta]^*(\pi \) is a unit) \( \implies \pi \)}
not prime, a contradiction. So \( \pi \) divides no other factor in the left-hand side of (3).

Since \( \pi \) divides \( z \), \( \pi^p \mid z^p \). No \( \pi \)-factor can divide other factors (of the left-hand side of (3)), so \( \pi^p \mid (x + y\zeta) \). By uniqueness of the decomposition of \( x + y\zeta \) into prime factors, and repeating the argument just done for \( \pi \) for the other factors, we find that

\[
x + y\zeta = ua^p,
\]

for some \( \alpha \in \mathbb{Z}[\zeta] \) and \( u \in \mathbb{Z}[\zeta]^* \). Write \( \alpha = a_0 + a_1\zeta + \cdots + a_{p-2}\zeta^{p-2} \). In \( \mathbb{Z}[\zeta]/(p) \), we have\(^2\)

\[
\left(\frac{\alpha}{(p)}\right)^p = a_0^p + a_1^p\zeta^p + \cdots + a_{p-2}^p\zeta^{(p-2)p} \equiv \sum_{i=0}^{p-2} a_i^p \equiv : a \in \mathbb{Z}/p\mathbb{Z}.
\]

By little Fermat, this implies

\[
x + y\zeta \equiv (p) ua^p \equiv (p) ua \equiv (p) ua^p
\]

hence (applying complex conjugation)

\[
x + y\bar{\zeta} \equiv (p) \bar{u}a^p.
\]

Noting that \( \bar{\zeta} = \zeta^{-1} \), multiplying by \( u/\bar{u} \) gives

\[
\frac{u}{\bar{u}}(x + y\zeta^{-1}) \equiv (p) ua^p \equiv (p) x + y\zeta^p,
\]

which by Kummer’s lemma becomes

\[
\pm\zeta^k(x + y\zeta^{-1}) \equiv (p) x + y\zeta
\]

so that \( p \mid \{x + y\zeta \mp \zeta^k x \mp \zeta^{k-1}y\} \) in \( \mathbb{Z}[\zeta] \). By uniqueness of the representation of elements of \( \mathbb{Z}[\zeta] \), this is impossible unless \( k = 1 \).

---

\(^2\)The first equality here is sometimes called the “freshman’s dream” identity. The basic point is that while in the freshman’s Calculus class \((x + y)^p = x^p + y^p\) is definitely wrong, in number theory it is true mod \( p \) because the \( \binom{p}{k} \)'s in the binomial expansion are divisible by \( p \). That’s the real reason why you aren’t allowed to take this course before Calculus.
(Recall $p \nmid x, y$.) Hence $p \mid \{(x \mp y) + \zeta(y \mp x)\} \implies p \mid x \pm y \implies x \equiv \pm y$.

Writing $x^p + (-z)^p = (-y)^p$, we obtain similarly $x \equiv \mp z$. If $x \equiv y$, then $2x^p \equiv x^p + y^p = z^p \equiv \mp x^p \implies p \mid 3x^p$ or $p \mid x^p$ (contradiction!). If $x \equiv -y$, then $0 = x^p - x^p \equiv x^p + y^p = z^p \implies p \mid z^p$ (contradiction!). (Note that the first contradiction wouldn’t go through if $p = 3$.) This completes the argument in Case 1.

Case 2: $\mathbb{Z}[\zeta]$ not a UFD. (i.e., $h_{\mathbb{Q}(\zeta_p)} > 1$) A variant of the above argument was proposed in general by Lamé in 1847. Liouville immediately noticed that if unique factorization didn’t hold, the proof was invalid; it turned out that Kummer had already published a proof that it didn’t. However, Kummer also pointed out that the proof could be salvaged somewhat by using the unique factorization property for “ideal numbers”, as described in the last section.

The question is how far “somewhat” goes. Clearly, we aren’t going to prove Fermat’s Last Theorem entirely. Wiles’s 1995 proof revolves around the modularity of elliptic curves over $\mathbb{Q}$ and requires much more sophisticated methods. So there must be a catch.

But we can still get nonexistence of solutions in some non-UFD cases. Write, in analogy to (3),

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

which is now a factorization into principal ideals. If some prime ideal $\wp$ contains/divides $(x + y\zeta)$, then it can’t contain/divide any other on the left-hand side of (4). (Otherwise $\wp \supset (z, yp)$ as before.) Using the unique factorization of ideals in $\mathbb{Z}[\zeta]$ into prime ideals, we get $(x + y\zeta) = I^p$, $I$ not necessarily principal.

Now suppose that $p$ is a regular prime, i.e.

$$p \nmid h_{\mathbb{Q}(\zeta_p)}.
$$

Then $[I] \neq 1 \in Cl(\mathbb{Q}(\zeta_p))$, hence by Lagrange $[I]^p \neq 1 \in Cl(\mathbb{Q}(\zeta_p))$, contradicting principality of $(x + y\zeta)$. (Here, we are using the fact
that an ideal is principal iff its class in $Cl(K)$ is trivial.) Therefore $I$ must be principal, i.e. $I = (\alpha)$. Once again, we have $(x + y\zeta) = (\alpha^p) \implies x + y\zeta = u\alpha^p$, and at this point we can just proceed as in Case 1.

**Kummer’s result.** Putting everything together, we arrive at

**Theorem 6 (Kummer, 1847).** There are no solutions with $x, y, z \in \mathbb{Z}\setminus\{0\}$ to (1) with $m$ divisible by 4 or a regular prime.

That is, we have proved Fermat’s Last Theorem for (in particular) all exponents up to the first regular prime, which is 37. Note how deeply we dug into the ideal structure of $\mathbb{Z}[\zeta]$ to deal with an equation ostensibly in rational integers!