CYCLOTOMIC FIELDS

CARL ERICKSON

Cyclotomic fields are an interesting laboratory for algebraic number theory because they are connected to fundamental problems - Fermat's Last Theorem for example - and also have relatively simple algebraic properties that makes them an excellent laboratory for results in algebraic number theory.

I will assume that you are familiar with basic algebraic number theory. Namely, the unique factorization into primes ideals, ideal class group, Dirichlet's unit theorem, regulators, complex and real embeddings into $\mathbb{C}$, and the decomposition of primes (splitting, inertial degrees, ramification), the concept of a 'place,' and the should all be familiar. I will state the analytic class number formula and stuff from class field theory that you don't need to be an expert on.

I intend to accomplish the following:

(1) List some basic properties of cyclotomic fields

(2) Prove Fermat's last theorem in a certain case

(3) Describe, according to time available, Kummer's criterion for when we are in such a case

Alright, let's get going.

1. Basic Properties of Cyclotomic Fields

We will soon focus on cyclotomic fields associated to prime or prime power cyclotomic fields, but some things can be said in general. We let μ_n be a primitive nth root of unity and $K_n = \mathbb{Q}(\mu_n)$.

One of the most fundamental properties of cyclotomic fields in terms of basic algebraic number theory is that its ring of integers is rather easy to describe.

Proposition 1. *We have*

$$\mathcal{O}_{K_n} = \mathbb{Z}[\mu],$$

whereas computing the ring of integers for a number field is very hard in general.

Galois groups of cyclotomic fields are similarly easy to handle.

Proposition 2. *The Galois group of $K_n/\mathbb{Q}$ is*

$$\mathrm{Gal}(K_n/\mathbb{Q}) \cong (\mathbb{Z}/n\mathbb{Z})^\times.$$

The ease of the isomorphism: $(\sigma : \mu \to \mu^a) \longrightarrow a$ makes this one of the first examples in Galois theory.

From this we have the nice consequence,

Corollary 3. *For any finite abelian group G, there exists some number field F such that $F/\mathbb{Q}$ is Galois and*

$$G \cong \mathrm{Gal}(F/\mathbb{Q}).$$

The inverse Galois problem asks whether such a statement holds when G is not necessarily abelian, and is much harder.

It's also easy to tell what the ramified primes are:

$$p \text{ ramifies in } K/\mathbb{Q} \iff p \mid n$$

And actually it's not very hard to say a good deal more about the decomposition of primes. For $(m, n) = 1$ let f_m be the order of m in $(\mathbb{Z}/n\mathbb{Z})^\times$, and recall $\phi(n) = |(\mathbb{Z}/n\mathbb{Z})^\times|$.

Theorem 4. *Suppose $p \nmid n$. Then p splits into $\phi(n)/f_p$ primes in K_n, each with inertia degree f_p.*

Corollary 5. *The prime p splits completely in $K_n/\mathbb{Q} \iff p \equiv 1 \pmod{n}$.*

Proposition 6 (From Class Field Theory)**.** *We have*

1. *The ray class field to the modulus $n\infty$ is the unique extension such that all ideals that are $\equiv 1 \pmod{n}$ split completely.*
2. *Every abelian extension of the rationals is contained in some ray class field of $\mathbb{Q}$*

Corollary 7 (Kronecker-Weber Theorem)**.** *Every abelian extension of $\mathbb{Q}$ is contained in some cyclotomic field K_n.*

Now let's specialize to the case $K = \mathbb{Q}(\mu_p)$ with p an odd prime. We could say some of these things about prime powers that we couldn't say about general n, but we're going to look mostly at the p case anyway, and we don't lose so very much. For starters, note that

$$[K : \mathbb{Q}] = \phi(p) = p - 1$$

and

$$\mathrm{Gal}(K/\mathbb{Q}) \cong \mathbb{Z}/(p-1)\mathbb{Z}.$$

We know that only p ramifies in K, but how does it ramify?

Proposition 8. *Only the prime p ramifies in K, and*

$$p\mathbb{Z}[\mu] = (p) = (\mu - 1)^{p-1}$$

Thus p is totally ramified in K.

We will often use the fact that $(1-\mu) = (1-\mu^i)$ is an equality of ideals for $p \nmid i$. This is evident because one can show that their quotient is a unit (which is also a fact we will use later), but I prefer to think of it as that the choice of μ among all primitive pth roots of unity is arbitrary.

2. A Case of Fermat's Last Theorem

This is virtually all we need to know in order to state and prove a case of Fermat's last theorem for regular primes.

Definition 9. *A odd prime p is called* regular *if the class group Cl_K of $K = \mathbb{Q}(\mu_p)$ has no p-torsion, i.e. the class number $|Cl_K|$ is prime to p.*

Theorem 10 (Kummer)**.** *Let p be a regular prime. Then Fermat's last theorem holds for p, i.e. there is no non-trivial integer solution to*

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

As a historical note, mathematicians ran into the issues of nonunique factorization in number fields when they tried to prove Fermat's last theorem while presuming that there was unique factorization in $K = \mathbb{Q}(\mu_p)$. Then Kummer developed his theory of "ideal numbers," which Dedekind later formulated into the theory of ideals. This theory allowed him to prove the above theorem. Note that when the class number of K is 1, then p is regular. Though there are conjecturally infinitely many regular primes, we can only prove that there are infinitely many irregular primes. And likewise, there are, unfortunately, only a few p such that K has unique factorization:

Theorem 11 (Montgomery, Uchida 1971)**.** *The ring of integers $\mathcal{O}_K$ is a UFD if and only if $p \leq 19$.*

Also, there are only 30 positive integral values of $m \neq 2 \pmod 4$ such that $\mathbb{Q}(\mu_m)$ has unique factorization (a result due to Malsey).

We will prove Fermat's last theorem for regular exponents in the case that $p \nmid xyz$ and $p \geq 5$. For $p = 3$ (and $p = 5$ as well) you can prove it with a simple congruence. Fermat's descent argument works for $p = 4$. The other case, when $p \mid z$, also follows from the supposition that p is regular, but this would take us too long.

Quite a few facts will need to be assembled before we can do the main proof of the theorem. The following facts will be very useful after we finish the proof as well.

Proposition 12. *These are facts about K.*

1. *K is a totally complex field, that is there are $r_1 = 0$ real embeddings of K into $\mathbb{C}$, and $r_2 = (p-1)/2$ conjugate pairs of complex embeddings.*
2. *The maximal (totally) real subfield of K is $K^+ = \mathbb{Q}(\mu + \mu^{-1})$, and its ring of integers is $\mathcal{O}_{K^+} = \mathbb{Z}[\mu + \mu^{-1}]$. We have $[K : K^+] = 2$.*
3. *K and K^+ have the same unit rank, ergo $\mathcal{O}_{K^+}^\times \hookrightarrow \mathcal{O}_K^\times$ has finite index.*

Remark: Facts like this hold for a more general class of fields called CM-fields.

Proof. To show (1): Note that every pth root of unity not equal to 1 is primitive, so the embeddings $K \hookrightarrow \mathbb{C}$ are given by $\mu \mapsto \mu^a$ for $a = 1, 2, \ldots, p-1$. Clearly each of these is not a real embedding. Thus they are complex embeddings, and as $\deg(K/\mathbb{Q}) = r_1 + 2r_2$, the result follows.

To show (2): Clearly $\mu + \mu^{-1}$ is real, so K^+ is a totally real field. It has index 2 in K because μ satisfies the irreducible polynomial

$$X^2 - (\mu + \mu^{-1})X + 2 = 0.$$

To show (3): By Dirichlet's unit theorem and (1), the unit rank of K is $r_1 + r_2 - 1 = (p-1)/2 - 1$. Since K^+ is totally real, its unit rank is its degree minus 1, which is also $(p-1)/2 - 1$. □

These facts are quite useful but we need a bit more in order to prove Fermat.

Proposition 13. *In fact, for any unit ε of $\mathbb{Z}[\mu]$, there exists a unit $\varepsilon_1 \in \mathcal{O}_{K^+}^\times$ and an integer r such that $\varepsilon = \mu^r \cdot \varepsilon_1$. Thus the index of the units of $\mathcal{O}_{K^+}$ in $\mathcal{O}_K$ is p.*

Proof. Choose ε as above and set $\alpha = \varepsilon/\bar{\varepsilon}$. Clearly α is an algebraic integer with absolute value 1; also, all of its conjugates have absolute value 1, since they commute with conjugation.

Claim An algebraic integer α whose Galois conjugates all have absolute value 1 must be a root of unity.

Proof. Say that the degree of α is d. Then each of its powers have degree no more than d. Let $f(x)$ be the minimal polynomial for a power of α. Then the ith coefficient of f is bounded by the binomial coefficient $\binom{i}{d}$ since all conjugates of α are bounded by 1. Therefore there are only finitely many such polynomials, ergo finitely many powers of α. □

The only roots of unity in K are $\pm\mu^a$, so $\varepsilon/\bar{\varepsilon} = \pm\mu^a$ for some a. We will now show that $\pm = +$.

Assume that $\pm = -$. Since ε is an integer, recall that $(p) = (\mu - 1)^{p-1}$ and write

$$\begin{aligned} \varepsilon &= b_0 + b_1\mu + \cdots + b_{p-2}\mu^{p-2} \\ &\equiv b_0 + b_1 + \cdots + b_{p-2} \pmod{\mu - 1}. \end{aligned}$$

Since $\bar{\varepsilon} = b_0 + b_1\mu^i + \cdots$, the same congruence is true for $\bar{\varepsilon}$. Therefore,

$$\varepsilon = -\mu^a\bar{\varepsilon} \equiv -\varepsilon \pmod{\mu - 1},$$

and $2\varepsilon \equiv 0 \pmod{\mu - 1}$. But this is impossible because $(\mu - 1)$ is relatively prime to 2 and ε is a unit.

Thus we conclude that $\varepsilon/\bar{\varepsilon} = \mu^a$. Letting $2r \equiv a \pmod{p}$ and $\varepsilon_1 = \mu^{-r}\varepsilon$, we get $\varepsilon = \mu^r\varepsilon_1$ and $\bar{\varepsilon}_1 = \varepsilon_1$, completing the proof. □

Not much longer now - we need these lemmas:

Lemma 14. *Suppose $\alpha = a_0 + a_1\mu + \cdots + a_{p-1}\mu^{p-1}$ with $a_i \in \mathbb{Z}$ (note the extra power of μ). If $a_i = 0$ for at least one i, then for $n \in \mathbb{Z}$, $n \mid \alpha \iff n \mid a_i$ for all i.*

Lemma 15. *Let $\alpha \in \mathbb{Z}[\mu]$. Then α^p is congruent modulo p to a rational integer. (Recall: $(p) = (1-\mu)^{p-1}$)*

Lemma 16. *If $x, y \in \mathbb{Z}$ are relatively prime, then the ideals*

$$(x + \mu^i y), \quad i = 0, 1, \ldots, p-1$$

in $\mathbb{Z}[\mu]$ are relatively prime.

Proof. (Lemma 14) Obvious. □

Proof. (Lemma 15) Let $\alpha = \sum_{i=0}^{p-2} a_i\mu^i$. Then

$$\alpha^p \equiv \sum_{i=0}^{p-2}(a_i\mu^i)^p \equiv \sum_{i=0}^{p-2} a_i \pmod{p}$$

as desired. □

Proof. (Lemma 16) Suppose $\wp$ is a prime ideal such that

$$\wp \mid (x + \mu^i y) \text{ and } \wp \mid (x + \mu^j y)$$

for some $i \neq j$. Then using the fact that $(1-\mu) = (1-\mu^a)$ for all $p \nmid a$, we have

$$\wp \mid (\mu^i y - \mu^j y) = (1-\mu)y$$

and

$$\wp \mid \left[\mu^j(x + \mu^i y) - \mu^i(x + \mu^j y)\right] = (1-\mu)x,$$

so since $(x, y) = 1$ it follows that $\wp \mid (1-\mu)$, ergo $\wp = (1-\mu)$.

To finish the lemma, we note that

$$x + y \equiv x + \mu^i y \equiv 0 \pmod{1-\mu}$$

and so since $x + y \in \mathbb{Z}$ and p is the rational prime divisible by $(1-\mu)$, we get

$$0 \equiv x + y \equiv x^p + y^p \equiv z^p \pmod{p}$$

which contradicts our assumption that $p \nmid xyz$. □

Now we are ready to prove Fermat's last theorem for the case that $p \nmid xyz$. Here is the basic idea, along with some of the facts we should gather together before we prove it.

The key idea is that we can argue by contradiction, factorizing a solution

$$z^p = x^p + y^p = (x+y)(x+\mu y)(x+\mu^2 y)\cdots(x+\mu^{-1}y)$$

and then have an equality of the principal ideals generated by the RHS and LHS.

Now we prove Fermat's last theorem for the exponent p, recalling that our assumptions are that $p \geq 5$ is a regular prime and $p \nmid xyz$.

Proof. Suppose that $x \equiv y \equiv -z \pmod{p}$. Then $-2z^p \equiv z^p \pmod{p}$, which cannot happen since $p \nmid 3z$. Thus we may rearrange the equation by flipping signs to get that $x \not\equiv y \pmod{p}$. This is a fact we will need later.

We have the equality of ideals

$$\prod_{i=0}^{p-1}(x + \mu^i y) = (z)^p.$$

By Lemma 16, the ideals on the left are relatively prime and therefore are each pth powers of an ideal, say

$$A_i^p = (x + \mu^i y).$$

Since p divides the class number of K, A_i is principal. Therefore for each i there exists an integer $\alpha_i \in \mathcal{O}_K$ such that $(x + \mu^i y) = (\alpha_i^p)$, so the two generators differ by a unit.

Let's focus on the case $i = 1$ and let ε be the unit such that $x+\mu y = \varepsilon\alpha^p$. By Proposition 13, we know that $\varepsilon = \mu^r \cdot \varepsilon_1$ for some $r \in \mathbb{Z}$ and ε_1 real. Now by Lemma 15, we may choose $a \in \mathbb{Z}$ such that $\alpha^p \equiv a \pmod{p}$. Thus

$$x + \mu y = \mu^r \varepsilon_1 \alpha^p \equiv \mu^r \varepsilon_1 a \pmod{p}$$

and the conjugate of that equivalence

$$x + \mu^{-1} y \equiv \mu^{-r} \varepsilon_1 a \pmod{p}.$$

Thus $x + \mu y$ and $x + \mu^{-1}$ differ by a factor of μ^{2r}, so

$$x + \mu y - \mu^{2r} x - \mu^{2r-1} y \equiv 0 \pmod{p}.$$

If $1, \mu, \mu^{2r}, \mu^{2r-1}$ are distinct, then since $p \geq 5$, Lemma 14 implies that $p \mid x, y$, which contradicts our assumptions. Thus they are not distinct. We know $1 \neq \mu$ and $\mu^{2r} \neq \mu^{2r-1}$, so we rule out these three cases to complete the proof:

$$\begin{aligned}
1 = \mu^{2r} \quad &\implies x + \mu y - x - \mu^{-1} y \equiv 0 \pmod{p} \\
&\implies \mu y(1 - \mu^{p-2}) \equiv 0 \pmod{p} \quad \times \\
1 = \mu^{2r-1} \quad &\implies (x - y)(1 - \mu) \equiv 0 \pmod{p} \quad \implies x \equiv y \pmod{p} \quad \times \\
\mu = \mu^{2r-1} \quad &\implies x(1 - \mu^2) \equiv 0 \pmod{p} \quad \implies p \mid x \quad \times .
\end{aligned}$$

□

We remark again that it is possible to prove Fermat's last theorem for a regular prime p in the case that $p \mid z$ via elementary means, though this case is admittedly more complicated.

3. When is a Prime Regular?

Kummer's criterion states a remarkable connection between values of the Riemann zeta function, essentially analytic quantities, and the p-divisibility of $h = h_p = |Cl_K|$.

Theorem 17 (Kummer)**.** *Let $\zeta(s)$ be the Riemann zeta function. Then p is irregular if and only if p divides the numerator of at least one of $\zeta(-1), \zeta(-3), \ldots, \zeta(4-p)$.*

If we define the Bernoulli numbers by

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

then in fact $\zeta(-n+1) = -B_n/n$ for $n = 1, 2, \ldots$ and it is not hard to see that B_n is zero for all odd n except $B_1 = -1/2$. Thus we can restate Kummer's criterion as

Corollary 18. *A prime p is irregular if and only if it divides the numerator of at least one of the Bernoulli numbers $B_2, B_4, \ldots, B_{p-3}$.*

Though we will state most of our results today in terms of Bernoulli numbers, we should keep in mind that analytic values are behind all types of Bernoulli numbers.

Here are a few examples:

$$B_2 = \frac{1}{6}, B_4 = \frac{-1}{30}, B_6 = \frac{1}{42}, B_8 = \frac{-1}{30}, B_{10} = \frac{5}{66}, B_{12} = \frac{-691}{2730}.$$

Thus we may easily verify that 691 is an irregular prime, and that $5, 7, 11, 13$ are regular.

One more topic that should be mentioned before going on is p-adic zeta and L-functions. Kummer proved his "Kummer congruences" (which will be useful later)

Theorem 19. *For all positive even $n \equiv m \neq 0 \pmod{p-1}$,*

$$\frac{B_n}{n} \equiv \frac{B_m}{m} \pmod{p}$$

is an equivalence of p-integral quantities.

In terms of zeta values, this implies that $\zeta(1-n) \equiv \zeta(1-m) \pmod{p}$ for such m, n. This is the first step toward showing that this ζ may be extended to a continuous function on p. All of the later parts of this talk have p-adic L-functions behind them, so I end up either quoting results or using overly elementary ways to accomplish what is needed.

Let us now set out to overview the proof of Kummer's criterion in the direction of $p \mid B_k \implies p \mid h$.

The key will be to relate arithmetic data of K to its maximal real subfield K^+, in the following progression:

(1) Write the Dedekind zeta functions $\zeta_K(s)$ for K and K^+ in terms of Dirichlet characters and their L-functions.

(2) Using Proposition 13, relate the regulators R_K and R_{K^+}. In fact, we will find that $R_K/R_{K^+} = 2^{(p-3)/2}$.

(3) Apply the analytic class number formula to the quotient $\zeta_K(s)/\zeta_{K^+}(s)$.

(4) Use the the conductor-discriminant formula and the functional equation for the L-functions to get cancellation in all factors of the equation except h/h^+ and $\prod_\chi L(0, \bar{\chi})$ for odd χ.

(5) Write these L-values as generalized Bernoulli numbers: in the same way that $\zeta(0) = -B_1$, get $L(0, \bar{\chi}) = -B_{1,\bar{\chi}}$. Namely,

$$\frac{h}{h^+} = 2p \prod_{\text{odd } \chi \in X_K} \left(-\frac{1}{2} B_{1,\chi}\right) = 2p \prod_{k=2 \text{ even}}^{p-1} \left(-\frac{1}{2} B_{1,\omega^{k-1}}\right)$$

where ω is a distinguished character called the Teichmuller character ($\omega(a) \equiv a \pmod{p}$ even though $\omega : \mathbb{Z} \to \mathbb{Q}(\mu_{p-1})$).

(6) Show that the class group of K^+ injects into that of K via the natural inclusion of ideals, so that h/h^+ is an integer and has arithmetic meaning (it's called the negative part of the class number, h^-).

(7) Use this formula for generalized Bernoulli numbers,

$$B_{1,\chi} = \frac{1}{p} \sum_{a=1}^{p} \chi(a) a,$$

and the special property of the Teichmuller character show that

$$B_{1,\omega^{p-2}} \equiv \frac{-1}{p} \mod \mathbb{Z}_p,$$

so

$$\frac{h}{h^+} \equiv \prod_{k=2, \text{ even}}^{p-3} \left(-\frac{1}{2} B_{1,\omega^{k-1}}\right) \pmod{p}$$

(8) Apply the Kummer congruence to get $B_{1,\omega^{k-1}} \equiv B_k/k \pmod{p}$ (all quantities being p-integral).

The above sketches the proof that $p \mid B_k$ for $k = 2, 4, \ldots, p-3$ implies that $p \mid h$, which is one direction of Kummer's criterion. To show the other direction, we prove that $p \mid h^+ \implies p \mid h^-$ and then apply the same congruence. This is accomplished by dealing with the even characters and showing that p-divisibility of their Bernoulli numbers is related to those of odd character Bernoulli numbers.

We complete this overview with a description of what Herbrand's theorem says. Let C be the class group of K and let $V = C/C^p$. This is a finite dimensional $\mathbb{F}_p$-vector space, on which $G = \mathrm{Gal}(K/\mathbb{Q})$ acts semi-simply. Therefore we may ask which characters $\omega^i \in G^\wedge$ occur in this action. That is, we may decompose it as

$$V = \bigoplus_{i \pmod{p-1}} V(\omega^i)$$

where

$$V(\omega^i) = \{v \in V \mid \sigma v = \chi^i(\sigma) v \text{ for all } \sigma \in G\}.$$

Herbrand proved

Theorem 20. *Let k be even. If $V(\omega^{1-k}) \neq 0$, then $p \mid B_k$.*

Ribet proved the converse by using properties of modular forms, the Shimura varieties one can attach to them, and then the Galois representations on the Tate module of that variety, which by the Eichler-Shimura relation are given by the action of absolute Frobenius elements.

4. Proving One Direction of Kummer's Criterion

We need to define several things first, for F a general number field.

Definition 21. *The* Dedekind zeta function *of F is*

$$\zeta_F(s) = \prod_{\wp}(1 - (N\wp)^{-s})^{-1},$$

where N is the absolute norm and the product is over the primes of K.

Definition 22. *A* Dirichlet character *is a homomorphism*

$$\chi : (\mathbb{Z}/n\mathbb{Z})^{\times} \to \mathbb{C}^{\times},$$

extended to $\mathbb{Z}$ by setting $\chi(m) = 0$ when $n \mid m$ and reducing to the appropriate residue class otherwise. Call χ even if $\chi(-1) = 1$, and odd if $\chi(-1) = -1$.

The following result quoted from the theory of Dirichlet characters.

Proposition 23. *Let F be a number field contained in $\mathbb{Q}(\mu_n)$ for some $n \in \mathbb{Z}^+$. Identify $G_n = \mathrm{Gal}(\mathbb{Q}(\mu_n)/\mathbb{Q})$ with $(\mathbb{Z}/n\mathbb{Z})^{\times}$ and let $X_F \leq G_n$ be the subgroup of Dirichlet characters whose kernel contains the subgroup of G_n fixing F. Then*

$$\zeta_F(s) = \prod_{\chi \in X_F} L(s, \chi)$$

where the L-function $L(s, \chi)$ is defined to be

$$L(s, \chi) = \sum_{n=0}^{\infty} \frac{\chi(n)}{n^s} = \prod_{q}(1 - \frac{\chi(q)}{q^s})^{-1}.$$

With these facts in place, we recall the analytic class number formula. Let F be a number field.

Theorem 24. *The Dedekind zeta function $\zeta_F(s)$ has a simple pole at $s = 1$ with residue*

$$\frac{2^{r_1}(2\pi)^{r_2} h_F R_F}{w_F \sqrt{|d(F)|}}.$$

In particular, if a number field F is as in the previous proposition, then $L(s, \chi = 1)$ has a simple pole at $s = 1$ with residue 1 and the remaining factors are non-zero, so the above is equal to

$$\prod_{1 \neq \chi \in X_F} L(1, \chi).$$

Let h^+ be the class number of the maximal real subfield $K^+ = \mathbb{Q}(\mu + \mu^{-1})$ of K. Recall that we want to prove one direction of Kummer's criterion by relating arithmetic data of K to that of K^+. In fact, what we will do is divide out their Dedekind zeta functions and calculate all other pieces of the ratio, leaving only that a ratio of class numbers h/h^+ depends on an expression involving L-values, which can then be related to Bernoulli numbers.

Note that because an odd character of $\mathrm{Gal}(K/\mathbb{Q})$ corresponds to complex conjugation (or alternatively because $[K : K^+] = 2$ uniquely), the subgroup of Dirichlet characters of $(\mathbb{Z}/n\mathbb{Z})^\times$ associated to K^+ is the group of even characters.

Let us also calculate: Roots of unity:

$$w_K = 2p \quad w_{K^+} = 2;$$

Regulators:
Recall that the regulator of a field F is

$$R_F = \left|\det(\delta_i \log|\sigma_i(\varepsilon_j)|)_{1\le i,j\le r}\right|,$$

where $\{\varepsilon_j\}$ is a set of generators for the units of $\mathcal{O}_F$ modulo roots of unity and the σ_i, and $r = r_1 + r_2 - 1$ of the $r+1$ embeddings $F \hookrightarrow \mathbb{C}$ (up to conjugate pair) are chosen to be σ_i. (The choice of which one is omitted does not matter) The δ_i factor is 1 for a real embedding σ_i and 2 for a representative σ_i of a pair of complex conjugate embeddings.

Proposition 13, shows that in our case, the units of K and K^+ only differ by roots of unity, so the elements $\{\varepsilon_j\}$ are exactly the same. All that differs is the δ_i in fact: since K is totally complex and K^+ is totally real, we have that

$$\frac{R_K}{R_{K^+}} = 2^r,$$

where r in this case is $(p-1)/2 - 1$.

Now we calculate and get:

$$\frac{\pi^{(p-1)/2}(h/h^+)2^{(p-1)/2}}{2p\sqrt{|d(K)/d(K^+)|}} = \lim_{s\to 1}\frac{\zeta_K(s)}{\zeta_{K^+}(s)} = \frac{\prod_{1\neq\chi\in X_K} L(1,\chi)}{\prod_{\chi\in X_F \text{ even}} L(1,\chi)} = \prod_{\chi \text{ odd}} L(1,\chi).$$

Now we apply the functional equation of L-functions for odd Dirichlet characters to get

$$L(1,\chi) = \frac{\tau(\chi)\pi}{i f_\chi} L(0,\bar\chi)$$

where $\tau(\chi)$ is the Gauss sum of χ and f_χ is the conductor of χ (the minimal modulus to which χ is a Dirichlet character - we let f be the conductor of the relevant character).

Since there are $(p-1)/2$ odd characters we find that the π factors cancel and

$$2^{(p-1)/2}\frac{h}{h^+} = \left(\frac{\sqrt{|d(K)/d(K^+)|}}{\prod_\chi (i f_\chi/\tau(\chi))}\right)\left(2p\prod_{\chi \text{ odd}} L(0,\bar\chi)\right)$$

By the conductor-discriminant formula, the left quantity in parentheses is 1. Now recall that if $\zeta(s)$ is the Riemann zeta function, $\zeta(0) = -B_1 = 1/2$. In just the same way, one may define generalized Bernoulli numbers for Dirichlet characters, and get a similar relation with the L-function associated to that character. Namely,

$$L(0, \chi) = -B_{1,\chi}.$$

Thus we have proved the following

Proposition 25.

$$h^- = \frac{h}{h^+} = 2p \prod_{odd\ \chi \in X_K} \left(-\frac{1}{2} B_{1,\chi} \right).$$

Since K/K^+ is ramified at p (and at ∞), it follows by class field theory that the class number of K^+ divides the class number of K. Moreover, the natural map of ideals from $\mathcal{O}_{K^+}$ to $\mathcal{O}_K$ descends to an injective map on class groups, so the quantity $h^- = h/h^+$ has a good deal of arithmetic meaning, and is a positive integer.

Now we have shown that a factor of h may be written as a product of generalized Bernoulli numbers. All that remains is to connect the generalized Bernoulli numbers with the usual ones that we first introduced.

The most simple a priori definition of generalized Bernoulli numbers (letting $f = f_\chi$) is

Definition 26.

$$\sum_{n=0}^{f} \frac{\chi(a) t e^{at}}{e^{ft} - 1} = \sum_{n=0}^{\infty} B_{n,\chi} \frac{t^n}{n!}.$$

We are concerned with these numbers when $n = 1$. As long as χ is not a trivial Dirichlet character, we have that

$$B_{1,\chi} = \frac{1}{f} \sum_{a=1}^{f} \chi(a) a.$$

Note that for any of our characters in question, $f = q$.

Now choose $\omega : (\mathbb{Z}/p\mathbb{Z})^\times \longrightarrow \mu_{p-1} \subset \mathbb{Q}(\mu_{p-1}) = K_{p-1} \hookrightarrow \mathbb{C}$ to be the generator of X_K such that

$$\omega(a) \equiv a \pmod{\wp}$$

for some fixed prime $\wp$ over p in K_{p-1} (NB: p splits completely in K_{p-1} by Corollary 5, so you can think about things modulo $\wp$ basically the same way that you think about things modulo p in $\mathbb{Z}$)

Now we use the congruence $\omega(n) \equiv n^p \pmod{\wp^2}$ to get that

$$pB_{1,\omega^{k-1}} = \sum_{n=1}^{p-1} n^{1+p(k-1)}.$$

On the other hand, we have (Borevich-Shafarevich p. 385)

$$pB_t \equiv \sum_{n=1}^{p-1} n^t$$

Since we chose $\wp$ over p arbitrarily we can then say that

$$pB_{1,\omega^{k-1}} \equiv pB_{1+p(k-1)}$$

Note that $1 + p(k-1) \equiv k \pmod{p-1}$ and so we can apply the Kummer congruence to conclude that

$$pB_{1,\omega^{k-1}} \equiv p\frac{B_k}{k}.$$

for even k.

Now let's compute the product in question:

$$h^- = 2p \prod_{\text{odd } \chi \in X_K} \left(-\frac{1}{2}B_{1,\chi}\right) = 2p \prod_{k=2 \text{ even}}^{p-1} \left(-\frac{1}{2}B_{1,\omega^{k-1}}\right)$$

since ω is odd (as $\omega(-1) \equiv -1 \pmod{p}$).

The $k = p-1$ term is somewhat exceptional since the character we end up with is ω^{-1}.

$$B_{1,\omega^{p-1-1}} = B_{1,\omega^{-1}} = \frac{1}{p}\sum_{a=1}^{p-1} a\omega^{-1}(a) \equiv \frac{p-1}{p} \mod \mathbb{Z}_p.$$

(This reflects the von Staudt-Clausen theorem) Therefore $(2p)(-\frac{1}{2}B_{1,\omega^{p-2}} \equiv 1 \pmod{p})$, and we end up with

$$h^- \equiv \prod_{k=2,\text{ even}}^{p-3} \left(-\frac{1}{2}B_{1,\omega^{k-1}}\right) \pmod{p}$$

which by our recent calculation can be written

$$h^- \equiv \prod_{k=2,\text{ even}}^{p-3} \left(-\frac{1}{2}\frac{B_k}{k}\right) = \prod_{k=2,\text{ even}}^{p-3} \left(-\frac{1}{2}\zeta(1-k)\right).$$

By the von Staudt-Clausen theorem, these B_k are p-integral, we are done. We have shown that

Theorem 27. *Say that p divides the numerator of B_k for some $k = 2, 4, \ldots, p-3$. Then p divides h^-, ergo p divides $h = h^+h^-$ and p is irregular.*

The converse statement, which would complete Kummer's criterion, follows upon showing that if $p \mid h+$, then $p \mid h^-$ as well. This involves character computations that are best presented with p-adic L-functions.